TAMU-CC Cybersecurity Control Standards Catalog

Appendix A – Optional Controls

PURPOSE: Appendix A contains optional or advisory controls based on best practices in the National Institute of Standards and Technology (NIST) Framework. Nothing in Appendix A should be considered mandatory or required. This is a resource guide to best practices and is supplemental information.

Access Control – 102 controls

AC-2(1) Automated System Account Management

Description

Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Support the management of system accounts using automated mechanisms.

AC-2(2) Automated Temporary and Emergency Account Management

Description

Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Automatically disable temporary and emergency accounts within seventy-two (72) hours of no longer being needed.

AC-2(3) Disable Accounts

Description

Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Implementation

Disable accounts within seventy-two (72) hours when the accounts:

1) Have expired;
2) Are no longer associated with a user or individual;
3) Are in violation of organizational policy; or
4) Have been inactive for ninety (90) days.

AC-2(4) Automated Audit Actions

Description

Account management audit records are defined in accordance with AU-2 and reviewed, analyzed, and reported in accordance with AU-6.

Related Controls

AU-2, AU-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Automatically audit account creation, modification, enabling, disabling, and removal actions.

AC-2(5) Inactivity Logout

Description

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related Controls

AC-11

Implementation

Require that users log out when reaching the end of shift or when expected inactivity period is over four (4) hours.

AC-2(6) Dynamic Privilege Management

Description

In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on runtime access control decisions facilitated by dynamic privilege management, such as attribute-based access control. While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and the operational needs of organizations. An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges. Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege changes, for example, when there are changes to encryption keys used for communications.

Related Controls

AC-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement dynamic privilege management capabilities when application support is available.

AC-2(8) Dynamic Account Management

Description

Approaches for dynamically creating, activating, managing, and deactivating system accounts rely on automatically provisioning the accounts at runtime for entities that were previously unknown. Organizations plan for the dynamic management, creation, activation, and deactivation of system accounts by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges.

Related Controls

AC-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Create, activate, manage, and deactivate system accounts dynamically.

AC-2(9) Restrictions on Use of Shared and Group Accounts

Description

Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Only permit the use of shared and group accounts that meet the following requirements:

1) Will not access controlled or confidential data; and
2) Access of device needed to serve public interest.

AC-2(10) Shared and Group Account Credential Change

Withdrawn: Incorporated into AC-2(k)

AC-2(11) Usage Conditions

Description

Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.

The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Enforce *[Assignment: circumstances and/or usage conditions]* for *[Assignment: system accounts]*.

AC-2(12) Account Monitoring for Atypical Usage

Description

Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behavior by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behavior of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls

AU-6, AU-7, CA-7, IR-8, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

1) Monitor system accounts for atypical usage ; and

2) Report atypical usage of system accounts to the Office of Information Security.

AC-2(13) Disable Accounts for High-risk Individuals

Description

Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or the Nation. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Related Controls

AU-6, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Disable accounts of individuals within thirty (30) minutes of discovery of significant risks.

AC-4 Information Flow Enforcement

Description

Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-3). Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between connected systems. Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message filtering capability based on message content. Organizations also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are

generally not available in commercial off the-shelf products. Information flow enforcement also applies to control plane traffic (e.g., routing and DNS).

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Related Controls

AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC4, SC-7, SC-16, SC-31

Implementation

The Office of Information Security (OIS) enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on security controls found in information flow control best practices.

AC-4(1) Object Security and Privacy Attributes

Description

Information flow enforcement mechanisms compare security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labeled Secret would be allowed to flow to a destination object labeled Secret, but an information object labeled Top Secret would not be allowed to flow to a destination object labeled Secret. A dataset of personally identifiable

information may be tagged with restrictions against combining with other types of datasets and, thus, would not be allowed to flow to the restricted dataset. Security and privacy attributes can also include source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security or privacy attributes can be used, for example, to control the release of certain types of information.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Use privacy attributes associated with source, and destination objects to enforce information flow control policies as a basis for flow control decisions.

AC-4(2) Processing Domains

Description

Protected processing domains within systems are processing spaces that have controlled interactions with other processing spaces, enabling control of information flows between these spaces and to/from information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, system processes are assigned to domains, information is identified by types, and information flows are controlled based on allowed information accesses (i.e., determined by domain and type), allowed signaling among domains, and allowed process transitions to other domains.

Related Controls

SC-39

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Use protected processing domains to enforce information flow control policies as a basis for flow control decisions.

AC-4(3) Dynamic Information Flow Control

Description

Organizational policies regarding dynamic information flow control include allowing or disallowing information flows based on changing conditions or mission or operational considerations. Changing conditions include changes in risk tolerance due to changes in the immediacy of mission or business needs, changes in the threat environment, and detection of potentially harmful or adverse events.

Related Controls

SI-4

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Enforce information flow control policies.

AC-4(4) Flow Control of Encrypted Information

Description

Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term encryption is extended to cover encoded data not recognized by filtering mechanisms.

Related Controls

SI-4

Implementation

Prevent encrypted information from bypassing information flow control mechanisms by:

1) decrypting the information;
2) blocking the flow of the encrypted information;
3) terminating communications sessions attempting to pass encrypted information;

AC-4(5) Embedded Data Types

Description

Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes inserting files as objects within other files and using compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Enforce limitations on embedding data types within other data types.

AC-4(6) Metadata

Description

Metadata is information that describes the characteristics of data. Metadata can include structural metadata describing data structures or descriptive metadata describing data content.
Enforcement of allowed information flows based on metadata enables simpler and more effective flow control. Organizations consider the trustworthiness of metadata regarding data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e.,

protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., employing sufficiently strong binding techniques with appropriate assurance).

Related Controls

AC-16, SI-7

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Enforce information flow control based on data categorization attributes.

AC-4(7) One-way Flow Mechanisms

Description

One-way flow mechanisms may also be referred to as a unidirectional network, unidirectional security gateway, or data diode. One-way flow mechanisms can be used to prevent data from being exported from a higher impact or classified domain or system while permitting data from a lower impact or unclassified domain or system to be imported.

Applicability

This Control applies to university information resources that store or process mission

critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Enforce one-way information flows through hardware-based flow control mechanisms.

AC-4(8) Security and Privacy Policy Filters

Description

Organization-defined security or privacy policy filters can address data structures and content. For example, security or privacy policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security or privacy policy filters for data content can check for specific words, enumerated values or data value ranges, and hidden content. Structured data permits the interpretation of data content by applications. Unstructured data refers to digital information without a data structure or with a data structure that does not facilitate the development of rule sets to address the impact or classification level of the information conveyed by the data or the flow enforcement decisions. Unstructured data consists of bitmap objects that are inherently non-language-based (i.e., image, video, or audio files) and textual objects that are based on written or printed languages. Organizations can implement more than one security or privacy policy filter to meet information flow control objectives.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk

mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

TAMU-CC shall:

1) Enforce information flow control using security or privacy policy filters as a basis for flow control decisions for information flows ; and
2) Block, strip, modify, or quarantine data after a filter processing failure in accordance with security or privacy policy.

AC-4(9) Human Reviews

Description

Organizations define security or privacy policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human review may be employed in lieu of or as a complement to automated security or privacy policy filtering. Human reviews may also be employed as deemed necessary by organizations.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information.
The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Enforce the use of human reviews for information flows under the following conditions:

1) Anomaly activity detected;
2) Data leak suspected;
3) Vendor report of exploitation.

AC-4(10) Enable and Disable Security or Privacy Policy Filters

Description

For example, as allowed by the system authorization, administrators can enable security or privacy policy filters to accommodate approved data types. Administrators also have the capability to select the filters that are executed on a specific data flow based on the type of data that is being transferred, the source and destination security domains, and other security or privacy relevant features, as needed.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Provide the capability for privileged administrators to enable security or privacy policy filters under the following conditions:

1) Troubleshooting filter logic;
2) Prevent spread of data leakage;
3) Enforce information data flow policies;

AC-4(11) Configuration of Security or Privacy Policy Filters

Description

Documentation contains detailed information for configuring security or privacy policy filters. For example, administrators can configure security or privacy policy filters to include the list of inappropriate words that security or privacy policy mechanisms check in accordance with the definitions provided by organizations.

Applicability

This Control applies to University information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Provide the capability for privileged administrators to configure security or privacy policy filters to support different security or privacy policies.

AC-4(12) Data Type Identifiers

Description

Data type identifiers include filenames, file types, file signatures or tokens, and multiple internal file signatures or tokens. Systems only allow transfer of data that is compliant with data type format specifications. Identification and validation of data types is based on defined specifications associated with each allowed data format. The filename and number alone are not used for data type identification. Content is validated syntactically and semantically against its specification to ensure that it is the proper data type

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, use data categorization attributes to validate data essential for information flow decisions.

AC-4(13) Decomposition into Policy-relevant Subcomponents

Description

Decomposing information into policy-relevant subcomponents prior to information transfer facilitates policy decisions on source, destination, certificates, classification, attachments, and other security- or privacy-related component differentiators. Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, decompose information into

policy-relevant subcomponents for submission to policy enforcement mechanisms.

AC-4(14) Security or Privacy Policy Filter Constraints

Description

Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security or privacy policy filters that restrict data structures include restricting file sizes and field lengths. Data content policy filters include encoding formats for character sets, restricting character data fields to only contain alpha-numeric characters, prohibiting special characters, and validating schema structures.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, implement security or privacy policy filters requiring fully enumerated formats that restrict data structure and content.

AC-4(15) Detection of Unsanctioned Information

Description

Unsanctioned information includes malicious code, information that is inappropriate for release from the source network, or executable code that could disrupt or harm the services or systems on the destination network.

Related Controls

SI-3

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, examine the information for the presence of unsanctioned information and prohibit the transfer of such information in accordance with the security or privacy policy.

AC-4(16) Information Transfers on Interconnected Systems

Withdrawn: Incorporated into AC-4

AC-4(17) Domain Authentication

Description

Attribution is a critical component of a security and privacy concept of operations. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals. Successful domain authentication requires that system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Attribution also allows organizations to better maintain the lineage of personally identifiable information processing as it flows through systems and can facilitate consent tracking, as well as correction, deletion, or access requests from individuals.

Related Controls

IA-2, IA-3, IA-9

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

TAMU-CC shall uniquely identify and authenticate source and destination points by:

1) Organization;
2) System;
3) Application;
4) Service;
5) Individual for information transfer.

AC-4(18) Security Attribute Binding

Withdrawn: Incorporated into AC-16

AC-4(19) Validation of Metadata

Description

All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection. Some organizations distinguish between metadata and data payloads (i.e., only the

data to which the metadata is bound). Other organizations do not make such distinctions and consider metadata and the data to which the metadata applies to be part of the payload.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, implement security or privacy policy filters on metadata.

AC-4(20) Approved Solutions

Description

Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries. The National Security Agency (NSA) National Cross Domain Strategy and Management Office provides a listing of approved cross-domain solutions.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Employ solutions in approved configurations to control the flow of information across security domains.

AC-4(21) Physical or Logical Separation of Information Flows

Description

Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable. Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

Related Controls

SC-32

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Separate information flows logically or physically using mechanisms and/or techniques to accomplish required separations.

AC-4(22) Access Only

Description

The system provides a capability for users to access each connected security domain without providing any mechanisms to allow users to transfer data or information between the different security domains. An example of an access-only solution is a terminal that provides a user access to information with different security classifications while assuredly keeping the information separate.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.

AC-4(23) Modify Non-releasable Information

Description

Modifying non-releasable information can help prevent a data spill or attack when information is transferred across security domains. Modification actions include masking, permutation, alteration, removal, or redaction.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, modify non-releasable information by implementing obfuscation.

AC-4(24) Internal Normalized Format

Description

Converting data into normalized forms is one of most of effective mechanisms to stop malicious attacks and large classes of data exfiltration.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring

that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.

AC-4(25) Data Sanitization

Description

Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile devices, CDs, and DVDs) or in hard copy form.

Related Controls

MP-6

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, sanitize data to minimize*:*

1) delivery of malicious content;
2) command and control of malicious code;
3) malicious code augmentation;
4) steganography-encoded data;
5) spillage of sensitive information in accordance with security and privacy policies.

AC-4(26) Audit Filtering Actions

Description

Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Content filtering actions and the results of filtering actions are recorded for individual messages to ensure that the correct filter actions were applied. Content filter reports are used to assist in troubleshooting actions by, for example, determining why message content was modified and/or why it failed the filtering process. Audit events are defined in AU-2 . Audit records are generated in AU-12.

Related Controls

AU-2, AU-3, AU-12

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.

AC-4(27) Redundant/independent Filtering Mechanisms

Description

Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. Redundant and independent content filtering eliminates a single point of failure filtering system. Independence is defined as the implementation of a content filter that uses a different code base and supporting libraries (e.g., two JPEG filters using different vendors' JPEG libraries) and multiple, independent system processes.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.

AC-4(28) Linear Filter Pipelines

Description

Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined policy. The use of linear content filter pipelines ensures that filter processes are non-bypassable and always invoked. In general, the use of parallel filtering architectures for content filtering of a single data type introduces bypass and non-invocation issues.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.

AC-4(29) Filter Orchestration Engines

Description

Content filtering is the process of inspecting information as it traverses a cross-domain solution and determines if the information meets a predefined security policy. An orchestration engine coordinates the sequencing of activities (manual and automated) in a content filtering process.

Errors are defined as either anomalous actions or unexpected termination of the content filter process. This is not the same as a filter failing content due to non-compliance with policy. Content filter reports are a commonly used mechanism to ensure that expected filtering actions are completed successfully.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, employ content filter orchestration engines to ensure that:

1) Content filtering mechanisms successfully complete execution without errors; and
2) Content filtering actions occur in the correct order and comply with security and privacy policy.

AC-4(30) Filter Mechanisms Using Multiple Processes

Description

The use of multiple processes to implement content filtering mechanisms reduces the likelihood of a single point of failure.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, implement content filtering mechanisms using multiple processes.

AC-4(31) Failed Content Transfer Prevention

Description

Content that failed filtering checks can corrupt the system if transferred to the receiving domain.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.

AC-4(32) Process Requirements for Information Transfer

Description

The processes transferring information between filter pipelines have minimum complexity and functionality to provide assurance that the processes operate correctly.

Applicability

This Control applies to university information resources that store or process mission critical and/or confidential information. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource data/owners, management personnel, and system administrators.

Implementation

When transferring information between different security domains, the process that transfers information between filter pipelines:

1) Does not filter message content;
2) Validates filtering metadata;
3) Ensures the content associated with the filtering metadata has successfully completed filtering; and
4) Transfers the content to the destination filter pipeline.

AC-6(1) Authorize Access to Security Functions

Description

Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists. Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related Controls

AC-17, AC-18, AC-19, AU-9, PE-2

Implementation

Authorize access for individuals and roles to:

1) security functions (deployed in hardware, software, and firmware); and
2) security-relevant information.

AC-6(2) Non-privileged Access for Nonsecurity Functions

Description

Requiring the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Related Controls

AC-17, AC-18, AC-19, PL-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Require that users of system accounts (or roles) with access to security functions or security-relevant information use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-6(3) Network Access to Privileged Commands

Description

Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Related Controls

AC-17, AC-18, AC-19

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Authorize network access to privileged commands only for compelling operational needs and document the rationale for such access in the security plan for the system.

AC-6(4) Separate Processing Domains

Description

Providing separate processing domains for finer-grained allocation of user privileges includes using virtualization techniques to permit additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying physical machine, implementing separate physical domains, and employing hardware or software domain separation mechanisms.

Related Controls

AC-4, SC-2, SC-3, SC-30, SC-32, SC-39

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide separate processing domains to enable finer-grained allocation of user privileges.

AC-6(5) Privileged Accounts

Description

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related Controls

IA-2, MA-3, MA-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Restrict privileged accounts on the system to *[Assignment: personnel or roles]*.

AC-6(6) Privileged Access by Non-organizational Users

Description

An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or

individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.

Related Controls

AC-18, AC-19, IA-2, IA-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit privileged access to the system by non-organizational users.

AC-6(7) Review of User Privileges

Description

The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related Controls

CA-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

TAMU-CC shall:

1) Review annually the privileges assigned to privileged accounts (.admin, .epadm) to validate the need for such privileges; and
2) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6(8) Privilege Levels for Code Execution

Description

In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent the following software from executing at higher privilege levels than users executing the software: *[Assignment: software]*.

AC-6(9) Log Use of Privileged Functions

Description

The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

Related Controls

AU-2, AU-3, AU-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Log the execution of privileged functions.

AC-6(10) Prohibit Non-privileged Users from Executing Privileged Functions

Description

Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Privileged functions that require protection from nonprivileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-3.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented.
The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent non-privileged users from executing privileged functions.

AC-7(1) Automatic Account Lock

Withdrawn: Incorporated into AC-7

AC-7(2) Purge or Wipe Mobile Device

Description

A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local,

nonremovable or removable data storage; and includes a self-contained power source. Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

Related Controls

AC-19, MP-5, MP-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Purge or wipe information from mobile devices based on purging or wiping requirements or techniques after ten (10) consecutive, unsuccessful device logon attempts.

AC-7(3) Biometric Attempt Limiting

Description

Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts for users based on organizationally defined factors.

Related Controls

IA-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Limit the number of unsuccessful biometric logon attempts to ten (10).

AC-7(4) Use of Alternate Authentication Factor

Description

The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.

Related Controls

IA-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

TAMU-CC shall:

1) Allow the use of authentication factors that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; and
2) Enforce a limit of ten (10) consecutive invalid logon attempts through use of the alternative factors by a user during a fifteen (*15) minute period*.

AC-9 Previous Logon Notification

Description

Previous logon notification is applicable to system access via human user interfaces and access to systems that occurs in other types of architectures. Information about the last successful logon allows the user to recognize if the date and time provided is not consistent with the user's last access.

Related Controls

AC-7, PL-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Notify the user, upon successful logon to the system, of the date and time of the last logon.

AC-9(1) Unsuccessful Logons

Description

Information about the number of unsuccessful logon attempts since the last successful logon allows the user to recognize if the number of unsuccessful logon attempts is consistent with the user's actual logon attempts.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.

AC-9(2) Successful and Unsuccessful Logons

Description

Information about the number of successful and unsuccessful logon attempts within a specified time period allows the user to recognize if the number and type of logon attempts are consistent with the user's actual logon attempts.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Notify the user, upon successful logon, of the number of *[Selection: successful logons; unsuccessful logon attempts; both]* during *[Assignment: time period]*.

AC-9(3) Notification of Account Changes

Description

Information about changes to security-related account characteristics within a specified time period allows users to recognize if changes were made without their knowledge.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Notify the user, upon successful logon, of changes to security-related characteristics or parameters during last seven (7) days.

AC-9(4) Additional Logon Information

Description

Organizations can specify additional information to be provided to users upon logon, including the location of the last logon. User location is defined as information that can be determined by systems, such as Internet Protocol (IP) addresses from which network logons occurred, notifications of local logons, or device identifiers.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Notify the user, upon successful logon, of the following additional information:

1) Date of last unsuccessful login;
2) IP of last unsuccessful login.

AC-10 Concurrent Session Control

Description

Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

Related Controls

SC-23

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

The information system limits the number of concurrent sessions for each non-privileged user to five (5) concurrent sessions for system accounts.

AC-11(1) Pattern-hiding Displays

Description

The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

AC-12 Session Termination

Description

Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10 , which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related Controls

MA-4, SC-10, SC-23

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Automatically terminate a user session after 8 hours.

AC-12(1) User-initiated Logouts

Description

Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to *[Assignment: information resources]*.

AC-12(2) Termination Message

Description

Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Display an explicit logout message to users indicating the termination of authenticated communications sessions.

AC-12(3) Timeout Warning Message

Description

To increase usability, notify users of pending session termination and prompt users to continue the session. The pending session termination time period is based on the parameters defined in the AC-12 base control.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Display an explicit message to users indicating that the session will end in fifteen (15) minutes.

Control Enhancements

AC-14(1) Necessary Uses

Withdrawn: Incorporated into AC-14

AC-15 Automated Marking

Withdrawn: Incorporated into MP-3

AC-16 Security and Privacy Attributes

Description

Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures, such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions that represent the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently or in conjunction with security attributes, represent the basic properties or characteristics of active or passive entities with respect to the management of personally identifiable information. Attributes can be either explicitly or implicitly associated with the information contained in organizational systems or system components. Attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, cause information to flow among objects, or change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of attributes to subjects and objects by a system is referred to as binding and is inclusive of setting the attribute value and the attribute type. Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control,

including data retention limits, permitted uses of personally identifiable information, and identification of personal information within data objects. Such enforcement occurs through organizational processes or system functions or mechanisms. The binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play important parts in the trust that organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. The content or assigned values of attributes can directly affect the ability of individuals to access organizational information. Organizations can define the types of attributes needed for systems to support missions or business functions. There are many values that can be assigned to a security attribute. By specifying the permitted attribute ranges and values, organizations ensure that attribute values are meaningful and relevant. Labeling refers to the association of attributes with the subjects and objects represented by the internal data structures within systems. This facilitates system-based enforcement of information security and privacy policies. Labels include classification of information in accordance with legal and compliance requirements (e.g., top secret, secret, confidential, controlled unclassified), information impact level; high value asset information, access authorizations, nationality; data life cycle protection (i.e., encryption and data expiration), personally identifiable information processing permissions, including individual consent to personally identifiable information processing, and contractor affiliation. A related term to labeling is marking. Marking refers to the association of attributes with objects in a human-readable form and displayed on system media. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. Security and privacy labels may have the same value as media markings (e.g., top secret, secret, confidential). See MP-3 (Media Marking).

Related Controls

AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

a. Provide the means to associate *security and privacy attributes* with *security and privacy attribute values* for information in storage, in process, and/or in transmission;

b. Ensure that the attribute associations are made and retained with the information;

c. Establish the following permitted security and privacy attributes from the attributes defined in

d. Determine the following permitted attribute values or ranges for each of the established *attribute values or ranges*;

e. Audit changes to attributes; and

f. Review *security and privacy attributes* for applicability *annually*.

AC-16(1) Dynamic Attribute Association

Description

Dynamic association of attributes is appropriate whenever the security or privacy characteristics of information change over time. Attributes may change due to information aggregation issues (i.e., characteristics of individual data elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), changes in the security category of information, or changes in security or privacy policies. Attributes may also change situationally.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Dynamically associate security and privacy attributes with *subjects and objects* in accordance with the following security and privacy policies as information is created and combined.

AC-16(2) Attribute Value Changes by Authorized Individuals

Description

The content or assigned values of attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.

AC-16(3) Maintenance of Attribute Associations by System

Description

Maintaining the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. The integrity of specific items, such as security configuration files, may be maintained through the use of an integrity monitoring mechanism that detects anomalies and changes that deviate from

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Maintain the association and integrity of *security and privacy attributes* to *subjects and objects*.

AC-16(4) Association of Attributes by Authorized Individuals

Description

Systems, in general, provide the capability for privileged users to assign security and privacy attributes to system-defined subjects (e.g., users) and objects (e.g., directories, files, and ports). Some systems provide additional capability for general users to assign security and privacy attributes to additional objects (e.g., files, emails). The association of attributes by authorized individuals is described in the design documentation. The support provided by systems can include prompting users to select security and privacy attributes to be associated with information objects, employing automated mechanisms to categorize information with attributes based on defined policies, or ensuring that the combination of the security or privacy attributes selected is valid.

Organizations consider the creation, deletion, or modification of attributes when defining auditable events.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide the capability to associate *security and privacy attributes* with *subjects and objects* by authorized individuals (or processes acting on behalf of individuals).

AC-16(5) Attribute Displays on Objects to Be Output

Description

System outputs include printed pages, screens, or equivalent items. System output devices include printers, notebook computers, video displays, smart phones, and tablets. To mitigate the risk of unauthorized exposure of information (e.g., shoulder surfing), the outputs display full attribute values when unmasked by the subscriber.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify *instructions* using *naming conventions*.

AC-16(6) Maintenance of Attribute Association

Description

Maintaining attribute association requires individual users (as opposed to the system) to maintain associations of defined security and privacy attributes with subjects and objects.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Require personnel to associate and maintain the association of *security and privacy attributes* with *subjects and objects* in accordance with *security and privacy policies*.

AC-16(7) Consistent Attribute Interpretation

Description

To enforce security and privacy policies across multiple system components in distributed systems, organizations provide a consistent interpretation of security and privacy attributes employed in access enforcement and flow enforcement decisions. Organizations can establish agreements and processes to help ensure that distributed system components implement attributes with consistent interpretations in automated access enforcement and flow enforcement actions.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.

AC-16(8) Association Techniques and Technologies

Description

The association of security and privacy attributes to information within systems is important for conducting automated access enforcement and flow enforcement actions. The association of such attributes to information (i.e., binding) can be accomplished with technologies and techniques that provide different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures that support cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement *techniques and technologies* in associating security and privacy attributes to information.

AC-16(9) Attribute Reassignment - Regrading Mechanisms

Description

A regrading mechanism is a trusted process authorized to re-classify and re-label data in accordance with a defined policy exception. Validated regrading mechanisms are used by organizations to provide the requisite levels of assurance for attribute reassignment activities. The validation is facilitated by ensuring that regrading mechanisms are single purpose and of limited function. Since security and privacy attribute changes can directly affect policy enforcement actions, implementing trustworthy regrading mechanisms is necessary to help ensure that such mechanisms perform in a consistent and correct mode of operation.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Change security and privacy attributes associated with information only via regrading mechanisms validated using *defined techniques or procedures*.

AC-16(10) Attribute Configuration by Authorized Individuals

Description

The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Thus, it is important for systems to be able to limit the ability to create or modify the type and value of attributes available for association with subjects and objects to authorized individuals only.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.

AC-17(1) Monitoring and Control

Description

Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2 . Audit events are defined in

Related Controls

AU-2, AU-6, AU-12, AU-14

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Employ automated mechanisms to monitor and control remote access methods.

AC-17(2) Protection of Confidentiality and Integrity Using Encryption

Description

Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related Controls

SC-8, SC-12, SC-13

Applicability

This Control applies to all individuals that remotely access Texas A&M University-Corpus Christi information resources from outside the Texas A&M University-Corpus Christi campus network. This includes students, faculty, and staff members as well as guest account users, vendors, and research partners.

Implementation

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(3) Managed Access Control Points

Description

Organizations consider the Trusted Internet Connections (TIC) initiative

Related Controls

SC-7

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Route remote accesses through authorized and managed network access control points.

AC-17(4) Privileged Commands and Access

Description

Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related Controls

AC-6, SC-12, SC-13

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

TAMU-CC shall:

1) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: *[Assignment: organization-defined needs]* ; and
2) Document the rationale for remote access in the security plan for the system.

AC-17(5) Monitoring for Unauthorized Connections

Withdrawn: Incorporated into SI-4

AC-17(6) Protection of Mechanism Information

Description

Remote access to organizational information by non-organizational entities can increase the risk of unauthorized use and disclosure about remote access mechanisms. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behavior (see PL-4) and access agreements (see PS-6).

Related Controls

AT-2, AT-3, PS-6

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Protect information about remote access mechanisms from unauthorized use and disclosure.

AC-17(7) Additional Protection for Security Function Access

Withdrawn: Incorporated into AC-3.10

AC-17(8) Disable Nonsecure Network Protocols

Withdrawn: Incorporated into CM-7

AC-17(9) Disconnect or Disable Access

Description

The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide the capability to disconnect or disable remote access to the system within thirty (30) minutes.

AC-17(10) Authenticate Remote Commands

Description

Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.

Related Controls

SC-12, SC-13, SC-23

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Implement *mechanisms* to authenticate *remote commands*.

AC-18(1) Authentication and Encryption

Description

Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related Controls

SC-8, SC-12, SC-13

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Protect wireless access to the system using authentication of (*users or devices)* and encryption.

AC-18(2) Monitoring Unauthorized Connections

Withdrawn: Incorporated into SI-4

AC-18(3) Disable Wireless Networking

Description

Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

AC-18(4) Restrict Configurations by Users

Description

Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

Related Controls

SC-7, SC-15

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

AC-18(5) Antennas and Transmission Power Levels

Description

Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Related Controls

PE-19

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

AC-19(1) Use of Writable and Portable Storage Devices

Withdrawn: Incorporated into MP-7

AC-19(2) Use of Personally Owned Portable Storage Devices

Withdrawn: Incorporated into MP-7

AC-19(3) Use of Portable Storage Devices with No Identifiable Owner

Withdrawn: Incorporated into MP-7

AC-19(4) Restrictions for Classified Information

Description

None.

Related Controls

CM-8, IR-4

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

TAMU-CC shall:

1) Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and
2) Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information:
    a. Connection of unclassified mobile devices to classified systems is prohibited;
    b. Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;
    c. Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and
    d. Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections information *security officials* , and if classified information is found, the incident handling policy is followed.
    e. Restrict the connection of classified mobile devices to classified systems in accordance with *security policies*.

AC-19(5) Full Device or Container-based Encryption

Description

Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related Controls

SC-12, SC-13, SC-28

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, or confidential information. The intended audience is all individuals who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Employ *full-device encryption* to protect the confidentiality and integrity of information on *mobile devices*.

AC-20(1) Limits on Authorized Use

Description

Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by

external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related Controls

CA-2

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: (a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or (b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20(2) Portable Storage Devices - Restricted Use

Description

Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related Controls

MP-7, SC-41

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using group policy enforcement.

AC-20(3) Non-organizationally Owned Systems - Restricted Use

Description

Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using data loss protection.

AC-20(4) Network Accessible Storage Devices - Prohibited Use

Description

Network-accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit the use of *network-accessible storage devices* in external systems.

AC-20(5) Portable Storage Devices - Prohibited Use

Description

Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.

Related Controls

MP-7, PL-4, PS-6, SC-41

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

AC-21 Information Sharing

Description

Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related Controls

AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

TAMU-CC:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for TAMU-CC authorized cloud sharing and on prem storage for controlled and confidential data categorizations; and
2. Employs cloud-based data loss prevention tools to assist users in making information sharing/collaboration decisions.

AC-21(1) Automated Decision Support

Description

Automated mechanisms are used to enforce information sharing decisions.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Employ *automated mechanisms* to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

AC-21(2) Information Search and Retrieval

Description

Information search and retrieval services identify information system resources relevant to an information need.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Implement information search and retrieval services that enforce *information sharing restrictions*.

AC-23 Data Mining Protection

Description

Data mining is an analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. Data storage objects include database records and database fields. Sensitive information can be extracted from data mining operations. When information is personally identifiable information, it may lead to unanticipated revelations about individuals and give rise to privacy risks. Prior to performing data mining activities, organizations determine whether such activities are authorized. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that address data mining requirements. Organizational personnel consult with the senior agency official for privacy and legal counsel

regarding such requirements. Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is available as open-source information residing on external sites, such as social networking or social media websites.

Related Controls

PM-12, PT-2

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Employ *techniques* for *data storage objects* to detect and protect against unauthorized data mining.

AC-24 Access Control Decisions

Description

Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when systems enforce access control decisions. While it is common to have access control decisions and access

enforcement implemented by the same entity, it is not required, and it is not always an optimal implementation choice. For some architectures and distributed systems, different entities may make access control decisions and enforce access.

Related Controls

AC-2, AC-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Establish procedures to ensure *access control decisions* are applied to each access request prior to access enforcement.

AC-24(1) Transmit Access Authorization Information

Description

Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information supporting security and privacy attributes. This is because in distributed systems, there are various access control decisions that need to be made, and different entities make these decisions in a serial fashion, each requiring those attributes to make the decisions. Protecting access authorization information ensures that such information cannot be altered, spoofed, or compromised during transmission.

Related Controls

AU-10

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Transmit *access authorization information* using *controls* to *systems* that enforce access control decisions.

AC-24(2) No User or Process Identity

Description

In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is simply not needed for access control decisions, and especially in the case of distributed systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish. MAC, RBAC, ABAC, and label-based control policies, for example, might not include user identity as an attribute.

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Enforce access control decisions based on *security or privacy attributes* that do not include the identity of the user or process acting on behalf of the user.

AC-25 Reference Monitor

Description

A reference monitor is a set of design requirements on a reference validation mechanism that, as a key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism is always invoked, tamper-proof, and small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable). Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are associated with data structures, such as records, buffers, communications ports, tables, files, and inter-process pipes. Reference monitors enforce access control policies that restrict access to objects based on the identity of subjects or groups to which the subjects belong. The system enforces the access control policy based on the rule set established by the policy. The tamper-proof property of the reference monitor prevents determined adversaries from compromising the functioning of the reference validation mechanism. The always invoked property prevents adversaries from bypassing the mechanism and violating the security policy. The smallness property helps to ensure completeness in the analysis and testing of the mechanism to detect any weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

Related Controls

AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resource owners and custodians.

Implementation

Implement a reference monitor for *access control policies* that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Awareness and Training – 11 controls

AT-2(1) Practical Exercises

Description

Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related

Controls

CA-2, CA-7,

CP-4, IR-3

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide practical exercises in literacy training that simulate events and incidents.

AT-2(2) Insider Threat

Description

Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

Related Controls

PM-12

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide literacy training on recognizing and reporting potential indicators of insider threat.

AT-2(3) Social Engineering and Mining

Description

Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-2(4) Suspicious Communications and Anomalous System Behavior

Description

A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or

contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using *indicators of malicious code*.

AT-2(5) Advanced Persistent Threat

Description

An effective way to detect advanced persistent threats (APT) and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide literacy training on the advanced persistent threat.

AT-2(6) Cyber Threat Environment

Description

Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.

Related Controls

RA-3

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

TAMU-CC shall:

1) Provide literacy training on the cyber threat environment; and
2) Reflect current cyber threat information in system operations.

AT-3(1) Environmental Controls

Description

Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating, ventilation, air conditioning, and power within the facility.

Related Controls

PE-1, PE-11, PE-13, PE-14, PE-15

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide *personnel* with initial and *annual* training in the employment and operation of environmental controls.

AT-3(2) Physical Security Controls

Description

Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.

Related Controls

PE-2, PE-3, PE-4

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide *personnel* with initial and *annual* training in the employment and operation of physical security controls.

AT-3(3) Practical Exercises

Description

Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear, or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide practical exercises in security and privacy training that reinforce training objectives.

AT-3(4) Suspicious Communications and Anomalous System Behavior

Withdrawn: Moved to AT-2.4

AT-3(5) Processing Personally Identifiable Information

Description

Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, {#18e71fec-c6fd-475a-925a-5d8495cf8455} statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Related Controls

PT-2, PT-3, PT-5, PT-6

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide *personnel* with initial and *annual* training in the employment and operation of personally identifiable information processing and transparency controls.

AT-5 Contacts with Security Groups and Associations

Withdrawn: Incorporated into PM-15

AT-6 Training Feedback

Description

Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. Therefore, it is important that senior managers are made aware of such situations so that they can take appropriate response actions. Training feedback supports the evaluation and update of organizational training described in n AT-2b and AT-3b.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide feedback on organizational training results to the following personnel annually:

1) Chief Compliance Officer
2) Chief Information Officer
3) Vice President of Finance
4) President of Unversity.

Audit and Accountability – 45 controls

AU-2(1) Compilation of Audit Records from Multiple Sources

Withdrawn: Incorporated into AU-12

AU-2(2) Selection of Audit Events by Component

Withdrawn: Incorporated into AU-12

AU-2(3) Reviews and Updates

Withdrawn: Incorporated into AU-2

AU-2(4) Privileged Functions

Withdrawn: Incorporated into AC-6.9

AU-3(1) Additional Audit Information

Description

The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Implementation

Generate audit records containing the following additional information: *[Assignment: additional information]*.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

AU-3(2) Centralized Management of Planned Audit Record Content

Withdrawn: Incorporated into PL-9

AU-3(3) Limit Personally Identifiable Information Elements

Description

Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls

RA-3

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment *elements*.

AU-4(1) Transfer to Alternate Storage

Description

Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU-9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Transfer audit logs *weekly* to a different system, system component, or media other than the system or system component conducting the logging.

AU-5(1) Storage Capacity Warning

Description

Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide a warning to *personnel* within twenty-four (24) hours when allocated audit log storage volume reaches ninety (90) *percentage* of repository maximum audit log storage capacity.

AU-5(2) Real-time Alerts

Description

Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide an alert within *twenty-four (24)* to *the Office of Information Security* when the following audit failure events occur:

1) Banner Grade Report
2) Financial Aid Report
3) OIS Daily Report
4) OIS Weekly Report

AU-5(3) Configurable Traffic Volume Thresholds

Description

Organizations have the capability to reject or delay the processing of network communications traffic if audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function. The rejection or delay response is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and *reject or delay* network traffic above those thresholds.

AU-5(4) Shutdown on Failure

Description

Organizations determine the types of audit logging failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit logging failure is not so severe that it warrants a complete shutdown of the system supporting the core organizational mission and business functions. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives.

Related Controls

AU-15

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Invoke a *full system shutdown, partial system shutdown, or degraded operational mode with limited mission or business functionality available* in the event of *audit logging failures*, unless an alternate audit logging capability exists.

AU-5(5) Alternate Audit Logging Capability

Description

Since an alternate audit logging capability may be a short-term protection solution employed until the failure in the primary audit logging capability is corrected, organizations may determine that the alternate audit logging capability need only provide a subset of the primary audit logging functionality that is impacted by the failure.

Related Controls

AU-9

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee is responsible for ensuring that the measures described in this Control are implemented.

Implementation

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements *alternate audit logging functionality*.

AU-6(1) Automated Process Integration

Description

Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

Related Controls

PM-7

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Integrate audit record review, analysis, and reporting processes using *automated mechanisms*.

AU-6(2) Automated Security Alerts

Withdrawn: Incorporated into SI-4

AU-6(3) Correlate Audit Record Repositories

Description

Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related Controls

AU-12, IR-4

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-6(4) Central Review and Analysis

Description

Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

Related Controls

AU-2, AU-12

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

AU-6(5) Integrated Analysis of Audit Records

Description

Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Related Controls

AU-12, IR-4

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Integrate analysis of audit records with analysis of *vulnerability scanning information, performance data, or system monitoring information with data/information collected from other sources* to further enhance the ability to identify inappropriate or unusual activity.

AU-6(6) Correlation with Physical Monitoring

Description

The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

AU-6(7) Permitted Actions

Description

Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Specify the permitted actions for each *[Selection (one or more): system process; role; user]* associated with the review, analysis, and reporting of audit record information.

AU-6(8) Full Text Analysis of Privileged Commands

Description

Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system

where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

Related Controls

AU-3, AU-9, AU-11, AU-12

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

AU-6(9) Correlation with Information from Nontechnical Sources

Description

Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record

information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Related Controls

PM-12

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

AU-6(10) Audit Level Adjustment

Withdrawn: Incorporated into AU-6

AU-7 Audit Record Reduction and Report Generation

Description

Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability

includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

Related Controls

AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4

AU-7(1) Automatic Processing

Description

Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content:

1) Date/Time
2) Source
3) User
4) Action
5) Event ID
6) Device

AU-7(2) Automatic Sort and Search

Withdrawn: Incorporated into AU-7.1

AU-8(1) Synchronization with Authoritative Time Source

Withdrawn: Moved to SC-45.1

AU-8(2) Secondary Authoritative Time Source

Withdrawn: Moved to SC-45.2

AU-9(1) Hardware Write-once Media

Description

Writing audit trails to hardware-enforced, write-once media applies to the initial generation of audit trails (i.e., the collection of audit records that represents the information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. Writing audit trails to hardware-enforced, write-once media does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes Compact Disc-Recordable (CD-R), Blu-Ray Disc Recordable (BD-R), and Digital Versatile Disc Recordable (DVD-R). In contrast, the use of switchable write-protection media, such as tape cartridges, Universal Serial Bus (USB) drives, Compact Disc Re-Writeable (CD-RW), and Digital Versatile Disc-Read Write (DVD-RW) results in write-protected but not write-once media.

Related Controls

AU-4, AU-5

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Write audit trails to hardware-enforced, write-once media.

AU-9(2) Store on Separate Physical Systems or Components

Description

Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Related Controls

AU-4, AU-5

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Store audit records *daily* in a repository that is part of a physically different system or system component than the system or component being audited.

AU-9(3) Cryptographic Protection

Description

Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Related Controls

AU-10, SC-12, SC-13

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

AU-9(4) Access by Subset of Privileged Users

Description

Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls

AC-5

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Authorize access to management of audit logging functionality to only *privileged and administrative users or roles*.

AU-9(5) Dual Authorization

Description

Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms (also known as two-person control) require the approval of two authorized individuals to execute audit functions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related Controls

AC-3

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Enforce dual authorization for *deletion* of *audit information*.

AU-9(6) Read-only Access

Description

Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Authorize read-only access to audit information to *non- administrative users or roles*.

AU-9(7) Store on Component with Different Operating System

Description

Storing auditing information on a system component running a different operating system reduces the risk of a vulnerability specific to the system, resulting in a compromise of the audit records.

Related Controls

AU-4, AU-5, AU-11, SC-29

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Store audit information on a component running a different operating system than the system or component being audited.

AU-10(1) Association of Identities

Description

Binding identities to the information support audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of attribute binding between the information producer and the information based on the security category of the information and other relevant risk factors.

Related Controls

AC-4, AC-16

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

TAMU-CC shall:

1) Bind the identity of the information producer with the information to enforce *strength of binding and non-repudiation in accordance with Audit and Accountability policies*; and
2) Provide the means for authorized individuals to determine the identity of the producer of the information.

AU-10(2) Validate Binding of Information Producer Identity

Description

Validating the binding of the information producer identity to the information prevents the modification of information between production and review. The validation of bindings can be achieved by, for example, using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls

AC-3, AC-4, AC-16

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

TAMU-CC shall:

1) Validate the binding of the information producer identity to the information annually; and
2) Perform mitigation *actions* in the event of a validation error.

AU-10(3) Chain of Custody

Description

Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each individual who handled the evidence, the date and time the evidence was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release or transfer function, the system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, maintaining the credentials of reviewers or releasers provides the organization with the means to identify who reviewed and released the information. In the case of automated reviews, it ensures that only approved review functions are used.

Related Controls

AC-4, AC-16

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.

AU-10(4) Validate Binding of Information Reviewer Identity

Description

Validating the binding of the information reviewer identity to the information at transfer or release points prevents the unauthorized modification of information between review and the transfer or release. The validation of bindings can be achieved by using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls

AC-4, AC-16

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

(a) Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between *[Assignment: security domains]* ; and (b) Perform *[Assignment: actions]* in the event of a validation error.

AU-10(5) Digital Signatures

Withdrawn: Incorporated into SI-7

AU-11(1) Long-term Retrieval Capability

Description

Organizations need to access and read audit records requiring long-term storage (on the order of years). Measures employed to help facilitate the retrieval of audit records include converting records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records.

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Employ *measures* to ensure that long-term audit records generated by the system can be retrieved.

AU-12(1) System-wide and Time-correlated Audit Trail

Description

Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Related Controls

AU-8, SC-45

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Compile audit records from *critical systems* into a system-wide (logical or physical) audit trail that is time-correlated to within *ten (10) seconds*.

AU-12(2) Standardized Formats

Description

Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

AU-12(3) Changes by Authorized Individuals

Description

Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

Related Controls

AC-3

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide and implement the capability for *[Assignment: individuals or roles]* to change the logging to be performed on *[Assignment: system components]* based on *[Assignment: selectable event criteria]* within *[Assignment: time thresholds]*.

AU-12(4) Query Parameter Audits of Personally Identifiable Information

Description

Query parameters are explicit criteria that an individual or automated system submits to a system to retrieve data. Auditing of query parameters for datasets that contain personally identifiable information augments the capability of an organization to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.

Applicability

This Control applies to all TAMU-CC information resources storing or accessing restricted or confidential information. The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.

AU-13 Monitoring for Information Disclosure

Description

Unauthorized disclosure of information is a form of data leakage. Open-source information includes social networking sites and code-sharing platforms and repositories. Examples of organizational information include personally identifiable information retained by the organization or proprietary information generated by the organization.

Related Controls

AC-22, PE-3, PM-12, RA-5, SC-7, SI-20

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

TAMU-CC shall:

1) Monitor *open-source information and information sites* for evidence of unauthorized disclosure of organizational information; and
2) If an information disclosure is discovered:

    a) Notify the Office of Information Security; and

    b) Take additional mitigating actions.

AU-13(1) Use of Automated Tools

Description

Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) or delegate.

Implementation

Monitor open-source information and information sites using *automated mechanisms*.

AU-13(2) Review of Monitored Sites

Description

Reviewing the current list of open-source information sites being monitored on a regular basis helps to ensure that the selected sites remain relevant. The review also provides the opportunity to add new open-source information sites with the potential to provide evidence of unauthorized disclosure of organizational information. The list of sites monitored can be guided and informed by threat intelligence of other credible sources of information.

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) or delegate.

Implementation

Review the list of open-source information sites being monitored *quarterly*.

AU-13(3) Unauthorized Replication of Information

Description

The unauthorized use or replication of organizational information by external entities can cause adverse impacts on organizational operations and assets, including damage to reputation. Such activity can include the replication of an organizational website by an adversary or hostile threat actor who attempts to impersonate the web-hosting organization. Discovery tools, techniques, and processes used to determine if external entities are replicating organizational information in an unauthorized manner include scanning external websites, monitoring social media, and training staff to recognize the unauthorized use of organizational information.

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) or delegate.

Implementation

Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

AU-14 Session Audit

Description

Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology. Organizations consider how session auditing can reveal information about individuals that may give rise to privacy risk as well as how to mitigate those risks. Because session auditing can impact system and network performance, organizations activate the capability under well-defined situations (e.g., the

organization is suspicious of a specific individual). Organizations consult with legal counsel, civil liberties officials, and privacy officials to ensure that any legal, privacy, civil rights, or civil liberties issues, including the use of personally identifiable information, are appropriately addressed.

Related Controls

AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

a. Provide and implement the capability for *security administrators* to *record, view, hear, or log* the content of a user session under approved investigations ; and

b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

AU-14(1) System Start-up

Description

The automatic initiation of session audits at startup helps to ensure that the information being captured on selected individuals is complete and not subject to compromise through tampering by malicious threat actors.

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Initiate session audits automatically at system start-up.

AU-14(2) Capture and Record Content

Withdrawn: Incorporated into AU-14

AU-14(3) Remote Viewing and Listening

Description

None.

Related Controls

AC-17

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.

AU-15 Alternate Audit Logging Capability

Withdrawn: Moved to AU-5.5

AU-16 Cross-organizational Audit Logging

Description

When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach. For example, maintaining the identity of individuals who request specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational audit logging simply captures the identity of individuals who issue requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations consider including processes for coordinating audit information requirements and protection of audit information in information exchange agreements.

Related Controls

AU-3, AU-6, AU-7, CA-3, PT-7

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Employ *methods* for coordinating *audit information* among external organizations when audit information is transmitted across organizational boundaries.

AU-16(1) Identity Preservation

Description

Identity preservation is applied when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

Related Controls

IA-2, IA-4, IA-5, IA-8

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Preserve the identity of individuals in cross-organizational audit trails.

AU-16(2) Sharing of Audit Information

Description

Due to the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit

records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only individuals' home organizations have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

Related Controls

IR-4, SI-4

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Provide cross-organizational audit information to *organizations* based on *cross-organizational sharing agreements*.

AU-16(3) Disassociability

Description

Preserving identities in audit trails could have privacy ramifications, such as enabling the tracking and profiling of individuals, but may not be operationally necessary. These risks could be further amplified when transmitting information across organizational boundaries. Implementing privacy enhancing cryptographic techniques can disassociate individuals from audit information and reduce privacy risk while maintaining accountability.

Applicability

The intended audience is information resource custodians who are responsible for the installation of new information resources, the operations of existing information resources, and individuals accountable for information resources security.

Implementation

Implement *measures* to disassociate individuals from audit information transmitted across organizational boundaries.

CA - Assessment, Authorization, and Monitoring – 16 controls

CA-2(1) Independent Assessors

Description

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. Assessor independence determination includes whether contracted assessment services have

sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is analogous to having independent SMEs involved in design reviews. When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be useable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) who has the authority to administer the information security functions for the entire institution and is responsible for assessing and reporting to the President the status and effectiveness of security controls under Texas Administrative Code 202.76, Security Control Standards Catalog [TAC 202.76(c)]. This Control is distinct from the unit security risk assessments described in RA-3 Risk Assessment.

Implementation

Employ independent assessors or assessment teams to conduct control assessments.

CA-2(2) Specialized Assessments

Description

Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy.

Organizations conduct specialized assessments in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development life cycle (e.g., during initial design, development, and unit testing).

Related Controls

PE-3, SI-2

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) who has the authority to administer the information security functions for the entire institution and is responsible for assessing and reporting to the President the status and effectiveness of security controls under Texas Administrative Code 202.76, Security Control Standards Catalog [TAC 202.76(c)]. This Control is distinct from the unit security risk assessments described in RA-3 Risk Assessment.

Implementation

Include as part of control assessments, annually, *announced*:

1) *in-depth monitoring, security instrumentation;*
2) *automated security test cases;*
3) *vulnerability scanning;*
4) *malicious user testing;*
5) *insider threat assessment;*
6) *performance and load testing; or*
7) *data leakage or data loss assessment*.

CA-2(3) Leveraging Results from External Organizations

Description

Organizations may rely on control assessments of organizational systems by other (external) organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform. The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization’s past experience with the organization that conducted the assessment, the reputation of the assessment organization, the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Accredited testing laboratories that support the Common Criteria Program m [ISO 15408-1], the NIST Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.

Related Controls

SA-4

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) who has the authority to administer the information security functions for the entire institution and is responsible for assessing and reporting to the President the status and effectiveness of security controls under Texas Administrative Code 202.76, Security Control Standards Catalog [TAC 202.76(c)]. This Control is distinct from the unit security risk assessments described in RA-3 Risk Assessment.

Implementation

Leverage the results of control assessments performed by *external organizations* on *systems* when the assessment meets *requirements*.

CA-3(1) Unclassified National Security System Connections

Withdrawn: Moved to SC-7.25

CA-3(2) Classified National Security System Connections

Withdrawn: Moved to SC-7.26

CA-3(3) Unclassified Non-national Security System Connections

Withdrawn: Moved to SC-7.27

CA-3(4) Connections to Public Networks

Withdrawn: Moved to SC-7.28

CA-3(5) Restrictions on External System Connections

Withdrawn: Moved to SC-7.5

CA-3(6) Transfer Authorizations

Description

To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies-via independent means- whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer

information also applies to control plane traffic (e.g., routing and DNS) and services (e.g., authenticated SMTP relays).

Related Controls

AC-2, AC-3, AC-4

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) who has the authority to administer the information security functions for the entire institution and is responsible for assessing and reporting to the President the status and effectiveness of security controls under Texas Administrative Code 202.76, Security Control Standards Catalog [TAC 202.76(c)]. This Control is distinct from the unit security risk assessments described in RA-3 Risk Assessment.

Implementation

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

CA-3(7) Transitive Information Exchanges

Description

Transitive or “downstream” information exchanges are information exchanges between the system or systems with which the organizational system exchanges information and other systems. For mission-essential systems, services, and applications, including high value assets, it is necessary to identify such information exchanges. The transparency of the controls or protection measures in place in such downstream systems connected directly or indirectly to organizational systems is essential to understanding the security and privacy risks resulting from those information exchanges. Organizational systems can inherit risk from downstream systems through transitive connections and information exchanges, which can make the organizational systems more susceptible to threats, hazards, and adverse impacts.

Related Controls

SC-7

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) who has the authority to administer the information security functions for the entire institution and is responsible for assessing and reporting to the President the status and effectiveness of security controls under Texas Administrative Code 202.76, Security Control Standards Catalog [TAC 202.76(c)]. This Control is distinct from the unit security risk assessments described in RA-3 Risk Assessment.

Implementation

TAMU-CC shall:

1) Identify transitive (downstream) information exchanges with other systems through the systems identified in
2) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.

CA-4 Security Certification

Withdrawn: Incorporated into CA-2

CA-5(1) Automation Support for Accuracy and Currency

Description

Using automated tools helps maintain the accuracy, currency, and availability of the plan of action and milestones and facilitates the coordination and sharing of security and privacy information

throughout the organization. Such coordination and information sharing help to identify systemic weaknesses or deficiencies in organizational systems and ensure that appropriate resources are directed at the most critical system vulnerabilities in a timely manner.

Applicability

The intended audience includes information resource owners and custodians.

Implementation

Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using *automated mechanisms]*.

CA-6(1) Joint Authorization - Intra-organization

Description

Assigning multiple authorizing officials from the same organization to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. The intra-organization joint authorization process is most relevant for connected systems, shared systems, and systems with multiple information owners.

Related Controls

AC-6

Applicability

The intended audience includes information resource owners and custodians.

Implementation

Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

CA-6(2) Joint Authorization - Inter-organization

Description

Assigning multiple authorizing officials, at least one of whom comes from an external organization, to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It implements the concepts of separation of duties and dual authorization as applied to the system authorization process. Employing authorizing officials from external organizations to supplement the authorizing official from the organization that owns or hosts the system may be necessary when the external organizations have a vested interest or equities in the outcome of the authorization decision. The inter-organization joint authorization process is relevant and appropriate for connected systems, shared systems or services, and systems with multiple information owners. The authorizing officials from the external organizations are key stakeholders of the system undergoing authorization.

Related Controls

AC-6

Applicability

The intended audience includes information resource owners and custodians.

Implementation

Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.

CA-7(1) Independent Assessment

Description

Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

CA-7(2) Types of Assessments

Withdrawn: Incorporated into CA-2

CA-7(3) Trend Analyses

Description

Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the organization or the Federal Government, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from Inspectors General or auditors.

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.

CA-7(5) Consistency Analysis

Description

Security and privacy controls are often added incrementally to a system. As a result, policies for selecting and implementing controls may be inconsistent, and the controls could fail to work together in a consistent or coordinated manner. At a minimum, the lack of consistency and coordination could mean that there are unacceptable security and privacy gaps in the system. At worst, it could mean that some of the controls implemented in one location or by one component are actually impeding the functionality of other controls (e.g., encrypting internal network traffic can

impede monitoring). In other situations, failing to consistently monitor all implemented network protocols (e.g., a dual stack of IPv4 and IPv6) may create unintended vulnerabilities in the system that could be exploited by adversaries. It is important to validate-through testing, monitoring, and analysis-that the implemented controls are operating in a consistent, coordinated, non-interfering manner.

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner:

1) Perform annual risk assessments; and
2) Annual Policy reviews.

CA-7(6) Automation Support for Monitoring

Description

Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions.

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Ensure the accuracy, currency, and availability of monitoring results for the system using *automated mechanisms*.

CA-8(1) Independent Penetration Testing Agent or Team

Description

Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-2(1) provides additional information on independent assessments that can be applied to penetration testing.

Related Controls

CA-2

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

CA-8(2) Red Team Exercises

Description

Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering based attacks. Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations. Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement:

1) Phishing
2) Penetration testing
3) OWASP top ten or subset

CA-8(3) Facility Penetration Testing

Description

Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.

Related Controls

CA-2, PE-3

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Employ a penetration testing process that includes annually *unannounced* attempts to bypass or circumvent controls associated with physical access points to the facility.

CA-9(1) Compliance Checks

Description

Compliance checks include verification of the relevant baseline configuration.

Applicability

The intended audience includes the Chief Information Security and Privacy Officer (CISPO), information resource owners and custodians.

Implementation

Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

Related Controls

CM-6

Configuration Management – 45 controls

CM-2(1) Reviews and Updates

Withdrawn: Incorporated into CM-2

CM-2(2) Automation Support for Accuracy and Currency

Description

Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-8(2) for organizations that combine system component inventory and baseline configuration activities.

Related Controls

CM-7, IA-3, RA-5

Applicability

The intended audience includes information resource owners and custodians; and pertains to information resources considered moderate or high impact.

Implementation

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using *automated mechanisms*.

CM-2(3) Retention of Previous Configurations

Description

Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Applicability

The intended audience includes information resource owners and custodians; and pertains to information resources considered moderate or high impact.

Implementation

Retain three (3) previous versions of baseline configurations of the system to support rollback.

CM-2(4) Unauthorized Software

Withdrawn: Incorporated into CM-7.4

CM-2(5) Authorized Software

Withdrawn: Incorporated into CM-7.5

CM-2(6) Development and Test Environments

Description

Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility. Configurations in the test environment mirror configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. Separate baseline configurations do not necessarily require separate physical environments.

Related Controls

CM-4, SC-3, SC-7

Applicability

The intended audience includes information resource owners and custodians; and pertains to information resources considered moderate or high impact.

Implementation

Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.

CM-2(7) Configure Systems and Components for High-risk Areas

Description

When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the {#mp} (Media Protection) family.

Related Controls

MP-4, MP-5

Applicability

The intended audience includes information resource owners and custodians; and pertains to information resources considered moderate or high impact.

Implementation

TAMU-CC shall:

1) Issue *systems or system components* with secure *configurations* to individuals traveling to locations that the organization deems to be of significant risk; and

2) Apply device sanitization to the systems or components when the individuals return from travel.

CM-3(1) Automated Documentation, Notification, and Prohibition of Changes

Description

None.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation

TAMU-CC shall use *automated mechanisms* to:

1) Document proposed changes to the system;
2) Notify *approval authorities* of proposed changes to the system and request change approval;
3) Highlight proposed changes to the system that have not been approved or disapproved within *ninety (90) days*;
4) Prohibit changes to the system until designated approvals are received;
5) Document all changes to the system; and
6) Notify *Change Advisory Management* when approved changes to the system are completed.

CM-3(3) Automated Change Implementation

Description

Automated tools can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation

Implement changes to the current system baseline and deploy the updated baseline across the installed base using *automated mechanisms*.

CM-3(4) Security and Privacy Representatives

Description

Information security and privacy representatives include system security officers, senior agency information security officers, senior agency officials for privacy, or system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization defined parameter reflects the change control elements defined by organizations in CM-3g.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation

Require *security and privacy representatives* to be members of the *configuration change control element*.

CM-3(5) Automated Security Response

Description

Automated security responses include halting selected system functions, halting system processing, and issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of university information resources that store or process mission critical and/or confidential information.

Implementation

Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner:

1) *Alert the Office of Information Security; and*
2) *Take mitigation actions if needed.*

CM-3(6) Cryptography Management

Description

The controls referenced in the control enhancement refer to security and privacy controls from the control catalog. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

Related Controls

SC-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: *[Assignment: controls]*.

CM-3(7) Review System Changes

Description

Indications that warrant a review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process.

Related Controls

AU-6, AU-7, CM-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation

Review changes to the system annually or when *circumstances* determine whether unauthorized changes have occurred.

CM-3(8) Prevent or Restrict Configuration Changes

Description

System configuration changes can adversely affect critical system security and privacy functionality. Change restrictions can be enforced through automated mechanisms.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation

Prevent or restrict changes to the configuration of the system under the following circumstances:

[Assignment: circumstances].

CM-4(1) Separate Test Environments

Description

A separate test environment requires an environment that is physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

Related Controls

SA-11, SC-7

Applicability

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Implementation

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

CM-4(2) Verification of Controls

Description

Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related Controls

SA-11, SC-3, SI-6

Applicability

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Implementation

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

CM-5(1) Automated Access Enforcement and Audit Records

Description

Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Related Controls

AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12

Applicability

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Implementation

(a) Enforce access restrictions using *automated mechanisms*; and

(b) Automatically generate audit records of the enforcement actions.

CM-5(2) Review System Changes

Withdrawn: Incorporated into CM-3.7

CM-5(3) Signed Components

Withdrawn: Moved to CM-14

CM-5(4) Dual Authorization

Description

Organizations employ dual authorization to help ensure that any changes to selected system components and information cannot occur unless two qualified individuals approve and implement such changes. The two individuals possess the skills and expertise to determine if the proposed changes are correct implementations of approved changes. The individuals are also accountable for the changes. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. System-level information includes operational procedures.

Related Controls

AC-2, AC-5, CM-3

Applicability

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Implementation

Enforce dual authorization for implementing changes to *[Assignment: organization-defined system components and system-level information]*.

CM-5(5) Privilege Limitation for Production and Operation

Description

In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

Related Controls

AC-2

Applicability

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Implementation

TAMU-CC shall:

1) Limit privileges to change system components and system-related information within a production or operational environment; and
2) Review and reevaluate privileges *annually*.

CM-5(6) Limit Library Privileges

Description

Software libraries include privileged programs.

Related Controls

AC-2

Applicability

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Implementation

Limit privileges to change software resident within software libraries.

CM-5(7) Automatic Implementation of Security Safeguards

Withdrawn: Incorporated into SI-7

CM-6(1) Automated Management, Application, and Verification

Description

Automated tools (e.g., hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related Controls

CA-7

Applicability

The intended audience includes information resource owners and custodians; and pertains to information resources considered moderate or high impact.

Implementation

Manage, apply, and verify configuration settings for *system components* using *automated mechanisms*.

CM-6(2) Respond to Unauthorized Changes

Description

Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or-in extreme cases-halting affected system processing.

Related Controls

IR-4, IR-6, SI-7

Applicability

The intended audience includes information resource owners and custodians; and pertains to information resources considered moderate or high impact.

Implementation

Take the following actions in response to unauthorized changes to *configuration settings*:

1) Alert the Office of Information Security; and
2) Revert to last known authorized configuration.

CM-6(3) Unauthorized Change Detection

Withdrawn: Incorporated into SI-7

CM-6(4) Conformance Demonstration

Withdrawn: Incorporated into CM-4

CM-7(1) Periodic Review

Description

Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer

technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related Controls

AC-18

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Review the system *annually* to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
2) Disable or remove *functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure*.

CM-7(2) Prevent Program Execution

Description

Prevention of program execution addresses organizational policies, rules of behavior, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles allowed to approve program execution, permitting or prohibiting

specific software programs, or restricting the number of program instances executed at the same time.

Related Controls

CM-8, PL-4, PL-9, PM-5, PS-6

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Prevent program execution in accordance with *policies, rules of behavior, and/or access agreements regarding:*

1) *software program usage and restrictions; and*
2) *rules authorizing the terms and conditions of software program usage*.

CM-7(3) Registration Compliance

Description

Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Ensure compliance with *registration requirements*.

CM-7(4) Unauthorized Software - Deny-by-exception

Description

Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

Related Controls

CM-6, CM-8, CM-10, PL-9, PM-5

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Identify *software programs*;
2) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and
3) Review and update the list of unauthorized software programs *annually*.

CM-7(5) Authorized Software - Allow-by-exception

Description

Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for

attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces, application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system startup. The identification of authorized URLs for websites is addressed in CA-3(5) and SC-7.

Related Controls

CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Identify *software programs*;
2) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
3) Review and update the list of authorized software programs *annually*.

CM-7(6) Confined Environments with Limited Privileges

Description

Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Related Controls

CM-11, SC-44

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: *[Assignment: user-installed software]*.

CM-7(7) Code Execution in Protected Environments

Description

Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.

Related Controls

CM-10, SC-44

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of the Office of Information Security when such code is:

1) Obtained from sources with limited or no warranty; and/or
2) Without the provision of source code.

CM-7(8) Binary or Machine Executable Code

Description

Binary or machine executable code applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain back doors or malware, and there may be no support available.

Related Controls

SA-5, SA-22

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and
2) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.

CM-7(9) Prohibiting The Use of Unauthorized Hardware

Description

Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential in order to provide adequate security.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Identify *hardware components*;
2) Prohibit the use or connection of unauthorized hardware components;
3) Review and update the list of authorized hardware components *annually*.

CM-8(1) Updates During Installation and Removal

Description

Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Related Controls

PM-16

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Update the inventory of system components as part of component installations, removals, and system updates.

CM-8(2) Automated Maintenance

Description

Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is

deemed reasonable. Automated maintenance can be achieved by the implementation of CM-2(2) for organizations that combine system component inventory and baseline configuration activities.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using *automated mechanisms*.

CM-8(3) Automated Unauthorized Component Detection

Description

Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components (see CM-7(9)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant in order to be detected since some types of components do not have or cannot support agents (e.g., IoT devices, sensors). Isolation can be achieved , for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as

Related Controls

AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Detect the presence of unauthorized hardware, software, and firmware components within the system using *automated mechanisms monthly*; and
2) Take the following actions when unauthorized components are detected:
    a. *disable network access by unauthorized components;*
    b. *isolate unauthorized components;*
    c. *notify the Office of Information Security.*

CM-8(4) Accountability Information

Description

Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Related Controls

AC-3

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Include in the system component inventory information, a means for identifying by *name. position, or role,* individuals responsible and accountable for administering those components.

CM-8(5) No Duplicate Accounting of Components

Withdrawn: Incorporated into CM-8

CM-8(6) Assessed Configurations and Approved Deviations

Description

Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

CM-8(7) Centralized Repository

Description

Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Provide a centralized repository for the inventory of system components.

CM-8(8) Automated Location Tracking

Description

The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. The use of tracking mechanisms can be coordinated with senior agency officials for privacy if there are implications that affect individual privacy.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Support the tracking of system components by geographic location using *automated mechanisms*.

CM-8(9) Assignment of Components to Systems

Description

System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall:

1) Assign system components to a system; and
2) Receive an acknowledgement from system owner of this assignment.

CM-9 Configuration Management Plan

Description

Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components

and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities. Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents. Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration-managed. As systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related Controls

CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

TAMU-CC shall develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures.
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management.
d. Is reviewed and approved by *Change Management* ; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-9(1) Assignment of Responsibility

Description

In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

CM-10(1) Open-source Software

Description

Open-source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open-source software is that it provides organizations with the ability to examine the source code. In some cases, there is an online community associated with the software that inspects, tests, updates, and reports on issues found in software on an ongoing basis. However, remediating vulnerabilities in open-source software may be problematic. There may also be licensing issues associated with open-source software, including the constraints on derivative use of such software. Open-source software that is available only in binary form may increase the level of risk in using such software.

Related Controls

SI-7

Applicability

The intended audience includes information resource owners and custodians; and pertains to all information resources.

Implementation

Establish the following restrictions on the use of open-source software: *[Assignment: restrictions]*.

CM-11(1) Alerts for Unauthorized Installations

Withdrawn: Incorporated into CM-8.3

CM-11(2) Software Installation with Privileged Status

Description

Privileged status can be obtained, for example, by serving in the role of system administrator.

Related Controls

AC-5, AC-6

Applicability

This Control applies to all University information resources. The information resource owner, or designee, is responsible for ensuring risk mitigation measures described in this Control are implemented.

Implementation

Allow user installation of software only with explicit privileged status.

CM-11(3) Automated Enforcement and Monitoring

Description

Organizations enforce and monitor compliance with software installation policies using automated mechanisms to more quickly detect and respond to unauthorized software installation which can be an indicator of an internal or external hostile attack.

Applicability

This Control applies to all University information resources. The information resource owner, or designee, is responsible for ensuring risk mitigation measures described in this Control are implemented.

Implementation

Enforce and monitor compliance with software installation policies using *automated mechanisms*.

CM-12 Information Location

Description

Information location addresses the need to understand where information is being processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and system components. The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see FIPS 199). The location of the information and system components is also a factor in the architecture and design of the system.

Related Controls

AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7

Applicability

This Control applies to all University information resources. The information resource owner, or designee, is responsible for ensuring risk mitigation measures described in this Control are implemented.

Implementation

a. Identify and document the location of *[Assignment: information]* and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

CM-12(1) Automated Tools to Support Information Location

Description

The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Applicability

This Control applies to all University information resources. The information resource owner, or designee, is responsible for ensuring risk mitigation measures described in this Control are implemented.

Implementation

Use automated tools to identify *[Assignment: information by information type]* on *[Assignment: system components]* to ensure controls are in place to protect organizational information and individual privacy.

CM-13 Data Action Mapping

Description

Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. A map of system data actions includes discrete data actions, elements of personally identifiable information being processed in the data actions, system components involved in the data actions, and the owners or operators of the system components. Understanding what personally identifiable information is being processed (e.g., the sensitivity of the personally identifiable information), how personally identifiable information is being processed (e.g., if the data action is visible to the individual or is processed in another part of the system), and by whom (e.g., individuals may have different privacy perceptions based on the entity that is processing the personally identifiable information) provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system. Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the organization is using. The development of this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system.

Related Controls

AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8

Applicability

This Control applies to all University information resources. The information resource owner, or designee, is responsible for ensuring risk mitigation measures described in this Control are implemented.

Implementation

Develop and document a map of system data actions.

CM-14 Signed Components

Description

Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Related Controls

CM-7, SC-12, SC-13, SI-7

Applicability

This Control applies to all University information resources. The information resource owner, or designee, is responsible for ensuring risk mitigation measures described in this Control are implemented.

Implementation

Prevent the installation of *[Assignment: organization-defined software and firmware components]* without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Contingency Planning – 40 controls

CP-2(1) Coordinate with Related Plans

Discussion

Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Coordinate contingency plan development with organizational elements responsible for related plans.

CP-2(2) Capacity Planning

Discussion

Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related Controls

PE-11, PE-12, PE-13, PE-14, PE-18, SC-5

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

CP-2(3) Resume Mission and Business Functions

Discussion

Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Plan for the resumption of *critical systems that support* mission and business functions within *forty-eight (48) hours* of contingency plan activation.

CP-2(4) Resume All Mission and Business Functions

Withdrawn: Incorporated into CP-2.3

CP-2(5) Continue Mission and Business Functions

Discussion

Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Plan for the continuance of critical mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

CP-2(6) Alternate Processing and Storage Sites

Discussion

Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary

processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Plan for the transfer of *critical* mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

CP-2(7) Coordinate with External Service Providers

Discussion

When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Related Controls

SA-9

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

CP-2(8) Identify Critical Assets

Discussion

Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.

Related Controls

CM-8, RA-9

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Identify critical system assets supporting *critical* mission and business functions.

CP-3(1) Simulated Events

Discussion

The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Applicability

This Control applies to information resource owners or designees who are responsible for mission critical information resources.

Implementation

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

CP-3(2) Mechanisms Used in Training Environments

Discussion

Operational mechanisms refer to processes that have been established to accomplish an organizational goal or a system that supports a particular organizational mission or business objective. Actual mission and business processes, systems, and/or facilities may be used to generate simulated events and enhance the realism of simulated events during contingency training.

Applicability

This Control applies to information resource owners or designees who are responsible for mission critical information resources.

Implementation

Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.

CP-4(1) Coordinate with Related Plans

Discussion

Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related Controls

IR-8, PM-8

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Coordinate contingency plan testing with organizational elements responsible for related plans.

CP-4(2) Alternate Processing Site

Discussion

Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

Related Controls

CP-7

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

TAMU-CC shall test the contingency plan at the alternate processing site:

1) To familiarize contingency personnel with the facility and available resources; and
2) To evaluate the capabilities of the alternate processing site to support contingency operations.

CP-4(3) Automated Testing

Discussion

Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, selecting more realistic test scenarios and environments, and effectively stressing the system and supported mission and business functions.

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Test the contingency plan using *[Assignment: automated mechanisms]*.

CP-4(4) Full Recovery and Reconstitution

Discussion

Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Related Controls

CP-10, SC-24

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

CP-4(5) Self-challenge

Discussion

Often, the best method of assessing system resilience is to disrupt the system in some manner. The mechanisms used by the organization could disrupt system functions or system services in many ways, including terminating or disabling critical system components, changing the configuration of system components, degrading critical functionality (e.g., restricting network bandwidth), or altering privileges. Automated, on-going, and simulated cyber-attacks and service disruptions can reveal unexpected functional dependencies and help the organization determine its ability to ensure resilience in the face of an actual cyber-attack.

Applicability

This Control applies to all mission critical information resources, University Essential IT Services, and additional resources as identified by the Chief Information Security and Privacy Officer (CISPO), in consultation with the Chief Information Office (CIO). The information resource owner or designee is responsible for ensuring planning processes described in this Control are implemented. Based on risk management considerations, the university's Chief Information Security and Privacy Officer may determine, in consultation with the CIO, that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Control

Employ *mechanisms* to *system or system component* to disrupt and adversely affect the system or system component.

CP-5 Contingency Plan Update

Withdrawn: Incorporated into CP-2

CP-6(1) Separation from Primary Site

Discussion

Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern.

For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls

RA-3

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6(2) Recovery Time and Recovery Point Objectives

Discussion

Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

CP-6(3) Accessibility

Discussion

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls

RA-3

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

CP-7 Alternate Processing Site

Discussion

Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls

CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

TAMU-CC shall:

1) Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of *system operations* for essential mission and business functions within *24 hours* when the primary processing capabilities are unavailable;

2) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

3) Provide controls at the alternate processing site that are equivalent to those at the primary site.

CP-7(1) Separation from Primary Site

Discussion

Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern.
For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls

RA-3

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(2) Accessibility

Discussion

Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls

RA-3

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7(3) Priority of Service

Discussion

Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the

availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

CP-7(4) Preparation for Use

Discussion

Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

Related Controls

CM-2, CM-6, CP-4

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

CP-7(5) Equivalent Information Security Safeguards

Withdrawn: Incorporated into CP-7

CP-7(6) Inability to Return to Primary Site

Discussion

There may be situations that preclude an organization from returning to the primary processing site such as if a natural disaster (e.g., flood or a hurricane) damaged or destroyed a facility and it was determined that rebuilding in the same location was not prudent.

Applicability

An alternate storage site is an integral part of a contingency plan and applies to all mission critical information resources, University Essential IT Services, and additional resources as noted. The information resource owner or designee is responsible for determining how the alternate storage site is utilized.

Implementation

Plan and prepare for circumstances that preclude returning to the primary processing site.

CP-8 Telecommunications Services

Discussion

Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8 . Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls

CP-2, CP-6, CP-7, CP-11, SC-7

Applicability:

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites.

Implementation

TAMU-CC shall establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential mission and business functions within the business impact analysis when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8(1) Priority of Service Provisions

Discussion

Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when

they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

Applicability

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites

Implementation

TAMU-CC shall:

1) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
2) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8(2) Single Points of Failure

Discussion

In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Applicability

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites

Implementation

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8(3) Separation of Primary and Alternate Providers

Discussion

Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Applicability

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites

Implementation

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

CP-8(4) Provider Contingency Plan

Discussion

Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to

satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related Controls

CP-3, CP-4

Applicability

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites

Implementation

TAMU-CC shall:

1) Require primary and alternate telecommunications service providers to have contingency plans;
2) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and
3) Obtain evidence of contingency testing and training by providers *annually*.

CP-8(5) Alternate Telecommunication Service Testing

Discussion

Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure that there is no degradation in organizational missions or functions.

Related Controls

CP-3

Applicability

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites

Control

Test alternate telecommunication services annually.

CP-9(1) Testing for Reliability and Integrity

.Discussion

Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls

CP-4

Applicability

This Control applies to university information resources that contain mission critical information, Essential IT Services, and additional resources as noted. The intended audience is all information resource owners or designees who are responsible for the support and operation of mission critical information resources. Based on risk management considerations and business functions, the information resource owner may determine that it would be appropriate to apply the requirements of this Control to information resources not meeting the definition of mission critical.

Implementation

Test backup information *quarterly* to verify media reliability and information integrity

CP-9(2) Test Restoration Using Sampling

Discussion

Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

Related Controls

CP-4

Applicability

This Control applies to university information resources that contain mission critical information, Essential IT Services, and additional resources as noted. The intended audience is all information resource owners or designees who are responsible for the support and operation of mission critical information resources. Based on risk management considerations and business functions, the

information resource owner may determine that it would be appropriate to apply the requirements of this Control to information resources not meeting the definition of mission critical.

Implementation

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

CP-9(4) Protection from Unauthorized Modification

Withdrawn: Incorporated into CP-9

CP-9(5) Transfer to Alternate Storage Site

Discussion

System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

Related Controls

CP-7, MP-3, MP-4, MP-5

Applicability

This Control applies to university information resources that contain mission critical information, Essential IT Services, and additional resources as noted. The intended audience is all information resource owners or designees who are responsible for the support and operation of mission critical information resources. Based on risk management considerations and business functions, the information resource owner may determine that it would be appropriate to apply the requirements of this Control to information resources not meeting the definition of mission critical.

Implementation

Transfer system backup information to the alternate storage site *consistent with the recovery time and recovery point objectives*.

CP-9(6) Redundant Secondary System

Discussion

The effect of system backup can be achieved by maintaining a redundant secondary system that mirrors the primary system, including the replication of information. If this type of redundancy is in place and there is sufficient geographic separation between the two systems, the secondary system can also serve as the alternate processing site.

Related Controls

CP-7

Applicability

This Control applies to university information resources that contain mission critical information, Essential IT Services, and additional resources as noted. The intended audience is all information resource owners or designees who are responsible for the support and operation of mission critical information resources. Based on risk management considerations and business functions, the information resource owner may determine that it would be appropriate to apply the requirements of this Control to information resources not meeting the definition of mission critical.

Implementation

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

CP-9(7) Dual Authorization for Deletion or Destruction

Discussion

Dual authorization ensures that deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting or destroying backup information possess the skills or expertise to determine if the proposed deletion or destruction of information reflects organizational policies and procedures. Dual authorization may also be known as twoperson control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related Controls

AC-3, AC-5, MP-2

Applicability

This Control applies to university information resources that contain mission critical information, Essential IT Services, and additional resources as noted. The intended audience is all information resource owners or designees who are responsible for the support and operation of mission critical information resources. Based on risk management considerations and business functions, the information resource owner may determine that it would be appropriate to apply the requirements of this Control to information resources not meeting the definition of mission critical.

Implementation

Enforce dual authorization for the deletion or destruction of *backup information*.

CP-9(8) Cryptographic Protection

Discussion

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system

backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls

SC-12, SC-13, SC-28

Applicability

This Control applies to university information resources that contain mission critical information, Essential IT Services, and additional resources as noted. The intended audience is all information resource owners or designees who are responsible for the support and operation of mission critical information resources. Based on risk management considerations and business functions, the information resource owner may determine that it would be appropriate to apply the requirements of this Control to information resources not meeting the definition of mission critical.

Implementation

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of *backup information*.

CP-10(1) Contingency Plan Testing

Withdrawn: Incorporated into CP-4

CP-10(2) Transaction Recovery

Discussion

Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Applicability

This Control applies to university information resources that are considered mission critical to the unit or an Essential IT Service to the university, and additional resources as noted. Based on risk management considerations, the university's Chief Information Security Privacy Officer (CISPO) may determine, in consultation with the Chief Information Officer (CIO), that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Implement transaction recovery for systems that are transaction-based.

CP-10(3) Compensating Security Controls

Withdrawn: ===== Control Addressed through tailoring.

CP-10(4) Restore Within Time Period

Discussion

Restoration of system components includes reimaging, which restores the components to known, operational states.

Related Controls

CM-2, CM-6

Applicability

This Control applies to university information resources that are considered mission critical to the unit or an Essential IT Service to the university, and additional resources as noted. Based on risk management considerations, the university's Chief Information Security Privacy Officer (CISPO) may determine, in consultation with the Chief Information Officer (CIO), that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Provide the capability to restore system components consistent with the recovery time and recovery point objectives from configuration-controlled and integrity-protected information representing a known, operational state for the components.

CP-10(5) Failover Capability

Withdrawn: Incorporated into SI-13

CP-10(6) Component Protection

Discussion

Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers, and other system software.

Related Controls

AC-3, AC-6, MP-2, MP-4, PE-3, PE-6

Applicability

This Control applies to university information resources that are considered mission critical to the unit or an Essential IT Service to the university, and additional resources as noted. Based on risk management considerations, the university's Chief Information Security Privacy Officer (CISPO) may determine, in consultation with the Chief Information Officer (CIO), that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Provide the capability to restore system components within consistent with the recovery time and recovery point objectives from configuration-controlled and integrity-protected information representing a known, operational state for the components.

CP-12 Safe Mode

Discussion

For systems that support critical mission and business functions-including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments)-organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated either automatically or manually, restricts the operations that systems can execute when those conditions are encountered. Restriction includes allowing only selected functions to execute that can be carried out under limited power or with reduced communications bandwidth.

Related Controls

CM-2, SA-8, SC-24, SI-13, SI-17

Applicability

This Control applies to university information resources that are considered mission critical to the unit or an Essential IT Service to the university, and additional resources as noted. Based on risk management considerations, the university’s Chief Information Security Privacy Officer (CISPO) may determine, in consultation with the Chief Information Officer (CIO), that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

When *conditions* are detected, enter a safe mode of operation with *restrictions*.

CP-13 Alternative Security Mechanisms

Discussion

Use of alternative security mechanisms supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. The mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ alternative or supplemental mechanisms enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, the alternative or supplemental mechanisms are only applied to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue one-time pads to senior executives, officials, and system administrators if multi-factor tokens-the standard means for achieving secure authentication- are compromised.

Related Controls

CP-2, CP-11, SI-13

Applicability

This Control applies to university information resources that are considered mission critical to the unit or an Essential IT Service to the university, and additional resources as noted. Based on risk management considerations, the university's Chief Information Security Privacy Officer (CISPO) may determine, in consultation with the Chief Information Officer (CIO), that it would be appropriate to apply the requirements of this Control to information resources not meeting the Glossary definition of mission critical.

Implementation

Employ *alternative or supplemental security mechanisms* for satisfying *security functions* when the primary means of implementing the security function is unavailable or compromised

Identification and Authentication – 44 controls

IA-2(3) Local Access to Privileged Accounts

Withdrawn: Incorporated into IA-2.1

IA-2(4) Local Access to Non-privileged Accounts

Withdrawn: Incorporated into IA-2.2

IA-2(5) Individual Authentication with Group Authentication

Description

Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

IA-2(6) Access to Accounts -separate Device

Description

The purpose of requiring a device that is separate from the system to which the user is attempting to gain access for one of the factors during multi-factor authentication is to reduce the likelihood of compromising authenticators or credentials stored on the system. Adversaries may be able to compromise such authenticators or credentials and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process.

Related Controls

AC-6

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Implement multi-factor authentication for *local, network, and remote* access to *privileged accounts and non-privileged accounts* such that:

1) One of the factors is provided by a device separate from the system gaining access; and
2) The device meets *strength of mechanism requirements*.

IA-2(7) Network Access to Non-privileged Accounts - Separate Device

Withdrawn: Incorporated into IA-2.6

IA-2(8) Access to Accounts - Replay Resistant

Description

Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or cryptographic authenticators.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Implement replay-resistant authentication mechanisms for access to *privileged accounts and non-privileged accounts.*

IA-2(9) Network Access to Non-privileged Accounts - Replay Resistant

Withdrawn: Incorporated into IA-2.8

IA-2(10) Single Sign-on

Description

Single sign-on enables users to log in once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add

multi-factor authentication for applications and systems (existing and new) that may not be able to natively support multi-factor authentication.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Provide a single sign-on capability for *system accounts and services*.

IA-2(11) Remote Access - Separate Device

Withdrawn: Incorporated into IA-2.6

IA-2(12) Acceptance of PIV Credentials

Description

Acceptance of Personal Identity Verification (PIV)-compliant credentials applies to organizations implementing logical access control and physical access control systems. PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. The adequacy and reliability of PIV card issuers are authorized using

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Accept and electronically verify Personal Identity Verification-compliant credentials.

IA-2(13) Out-of-band Authentication

Description

Out-of-band authentication refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path) is used to identify and authenticate users or devices and is generally the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. Out-of-band authentication can be used to mitigate actual or suspected

Related Controls

IA-10, IA-11, SC-37

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Implement the following out-of-band authentication mechanisms under *[Assignment: conditions]*: *[Assignment: out-of-band authentication]*.

IA-3 Device Identification and Authentication

Description

Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., Media Access Control [MAC], Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Related Controls

AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Uniquely identify and authenticate *devices* before establishing a *local, remote, or network* connection.

IA-3(1) Cryptographic Bidirectional Authentication

Description

A local connection is a connection with a device that communicates without the use of a network. A network connection is a connection with a device that communicates through a network. A remote connection is a connection with a device that communicates through an external network. Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk.

Related Controls

SC-8, SC-12, SC-13

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Authenticate *devices* before establishing *local, remote, and network]* connection using bidirectional authentication that is cryptographically based.

IA-3(2) Cryptographic Bidirectional Network Authentication

Withdrawn: Incorporated into IA-3.1

IA-3(3) Dynamic Address Allocation

Description

The Dynamic Host Configuration Protocol (DHCP) is an example of a means by which clients can dynamically receive network address assignments.

Related Controls

AU-2

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

TAMU-CC shall:

1) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with *lease information and lease duration*; and
2) Audit lease information when assigned to a device.

IA-3(4) Device Attestation

Description

Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Device attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices.

Related Controls

CM-2, CM-3, CM-6

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Handle device identification and authentication based on attestation by *configuration management process*.

IA-4(1) Prohibit Account Identifiers as Public Identifiers

Description

Prohibiting account identifiers as public identifiers applies to any publicly disclosed account identifier used for communication such as, electronic mail and instant messaging. Prohibiting the use of systems account identifiers that are the same as some public identifier, such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers. Prohibiting account identifiers as public identifiers without the implementation of other supporting controls only complicates guessing of identifiers. Additional protections are required for authenticators and credentials to protect the account.

Related Controls

AT-2, PT-7

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.

IA-4(2) Supervisor Authorization

Withdrawn: Incorporated into IA-12.1

IA-4(3) Multiple Forms of Certification

Withdrawn: Incorporated into IA-12.2

IA-4(4) Identify User Status

Description

Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Manage individual identifiers by uniquely identifying each individual as *characteristics*.

IA-4(5) Dynamic Management

Description

In contrast to conventional approaches to identification that presume static accounts for preregistered users, many distributed systems establish identifiers at runtime for entities that were previously unknown. When identifiers are established at runtime for previously unknown entities, organizations can anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate credentials and related identifiers are essential.

Related Controls

AC-16

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Manage individual identifiers dynamically in accordance with *dynamic identifier policy*.

IA-4(6) Cross-organization Management

Description

Cross-organization identifier management provides the capability to identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

Related Controls

AU-16, IA-2, IA-5

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Coordinate with the following external organizations for cross-organization management of identifiers.

IA-4(7) In-person Registration

Withdrawn: Incorporated into IA-12.4

IA-4(8) Pairwise Pseudonymous Identifiers

Description

A pairwise pseudonymous identifier is an opaque unguessable subscriber identifier generated by an identity provider for use at a specific individual relying party. Generating distinct pairwise pseudonymous identifiers with no identifying information about a subscriber discourages subscriber activity tracking and profiling beyond the operational requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party except in situations where relying parties can show a demonstrable relationship justifying an operational need for correlation, or all parties consent to being correlated in such a manner.

Related Controls

IA-5

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Generate pairwise pseudonymous identifiers.

IA-4(9) Attribute Maintenance and Protection

Description

For each of the entities covered in IA-2, IA-3, IA-8, and IA-9, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Maintain the attributes for each uniquely identified individual, device, or service in *protected central storage*.

IA-5(1) Password-based Authentication

Description

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing

usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Related Controls

IA-6

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

For password-based authentication TAMU-CC shall:

1) Maintain a list of commonly-used, expected, or compromised passwords and update the list *quarterly* and when organizational passwords are suspected to have been compromised directly or indirectly;
2) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
3) Transmit passwords only over cryptographically-protected channels;
4) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

5) Require immediate selection of a new password upon account recovery;
6) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
7) Employ automated tools to assist the user in selecting strong password authenticators; and
8) Enforce the following composition and complexity rules: *composition and complexity rules*.

IA-5(2) Public Key-based Authentication

Description

Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

Related Controls

IA-3, SC-17

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

TAMU-CC shall:

1) For public key-based authentication:

a. Enforce authorized access to the corresponding private key; and
b. Map the authenticated identity to the account of the individual or group; and

2) When public key infrastructure (PKI) is used:
a. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
b. Implement a local cache of revocation data to support path discovery and validation.

IA-5(3) In-person or Trusted External Party Registration

Withdrawn: Incorporated into IA-12.4

IA-5(4) Automated Support for Password Strength Determination

Withdrawn: Incorporated into IA-5.1

IA-5(5) Change Authenticators Prior to Delivery

Description

Changing authenticators prior to the delivery and installation of system components extends the requirement for organizations to change default authenticators upon system installation by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to developers of commercial off-the-shelf information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource

owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

IA-5(6) Protection of Authenticators

Description

For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related Controls

RA-2

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-5(7) No Embedded Unencrypted Static Authenticators

Description

In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators.

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

IA-5(8) Multiple System Accounts

Description

When individuals have accounts on multiple systems and use the same authenticators such as passwords, there is the risk that a compromise of one account may lead to the compromise of other accounts. Alternative approaches include having different authenticators (passwords) on all systems, employing a single sign-on or federation mechanism, or using some form of one-time passwords on all systems. Organizations can also use rules of behavior (see PL-4) and access agreements (see PS-6) to mitigate the risk of multiple system accounts.

Related Controls

PS-6

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Implement *security controls* to manage the risk of compromise due to individuals having accounts on multiple systems.

IA-5(9) Federated Credential Management

Description

Federation provides organizations with the capability to authenticate individuals and devices when conducting cross-organization activities involving the processing, storage, or transmission of information. Using a specific list of approved external organizations for authentication helps to ensure that those organizations are vetted and trusted.

Related Controls

AU-7, AU-16

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Use the following external organizations to federate credentials: *[Assignment: external organizations]*.

IA-5(10) Dynamic Credential Binding

Description

Authentication requires some form of binding between an identity and the authenticator that is used to confirm the identity. In conventional approaches, binding is established by preprovisioning both the identity and the authenticator to the system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the system. New authentication techniques allow the binding between the identity and the authenticator to be implemented external to a system. For example, with smartcard credentials, the identity and authenticator are bound together on the smartcard. Using these credentials, systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

Related Controls

AU-16, IA-5

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Bind identities and authenticators dynamically using the following rules: *[Assignment: binding rules]*.

IA-5(11) Hardware Token-based Authentication

Withdrawn: Incorporated into IA-2.1, IA-2.2

IA-5(12) Biometric Authentication Performance

Description

Unlike password-based authentication, which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide exact matches. Depending on the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and the stored biometric that serves as the basis for comparison. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system.

Related Controls

AC-7

Implementation

For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements *biometric quality requirements*.

IA-5(13) Expiration of Cached Authenticators

Description

Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Prohibit the use of cached authenticators after one hundred eighty (180) days.

IA-5(14) Managing Content of PKI Trust Stores

Description

An organization-wide methodology for managing the content of PKI trust stores helps improve the accuracy and currency of PKI-based authentication credentials across the organization.

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.

IA-5(15) Gsa-approved Products and Services

Description

General Services Administration (GSA)-approved products and services are products and services that have been approved through the GSA conformance program, where applicable, and posted to the GSA Approved Products List. GSA provides guidance for teams to design and build functional and secure systems that comply with Federal Identity, Credential, and Access Management (FICAM) policies, technologies, and implementation patterns.

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Use only General Services Administration-approved products and services for identity, credential, and access management.

IA-5(16) In-person or Trusted External Party Authenticator Issuance

Description

Issuing authenticators in person or by a trusted external party enhances and reinforces the trustworthiness of the identity proofing process.

Related Controls

IA-12

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Require that the issuance of *[Assignment: types of and/or specific authenticators]* be conducted *in person or by a trusted external party* before a *registration authority* with authorization by *personnel or roles*.

IA-5(17) Presentation Attack Detection for Biometric Authenticators

Description

Biometric characteristics do not constitute secrets. Such characteristics can be obtained by online web accesses, taking a picture of someone with a camera phone to obtain facial images with or without their knowledge, lifting from objects that someone has touched (e.g., a latent fingerprint), or capturing a high-resolution image (e.g., an iris pattern). Presentation attack detection technologies including liveness detection, can mitigate the risk of these types of attacks by making it difficult to produce artifacts intended to defeat the biometric sensor.

Related Controls

AC-7

Applicability

This Control also applies to any other entity that uses university information resources that require authentication. The intended audiences are university employees who are required to ensure that password-based authentication procedures are followed (e.g., unit heads, information resource owners and custodians); and those individuals who need to be aware of the procedures (e.g., non-technical university employees, staff, faculty, student, guest, or visitor).

Implementation

Employ presentation attack detection mechanisms for biometric-based authentication.

IA-5(18) Password Managers

Description

For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords (see

Implementation

TAMU-CC shall:

1) Employ *password managers* to generate and manage passwords; and
2) Protect the passwords using *controls*.

IA-8(1) Acceptance of PIV Credentials from Other Agencies

Description

Acceptance of Personal Identity Verification (PIV) credentials from other federal agencies applies to both logical and physical access control systems. PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidelines. The adequacy and reliability of PIV card issuers are addressed and authorized using

Related Controls

PE-3

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

IA-8(2) Acceptance of External Authenticators

Description

Acceptance of only NIST-compliant external authenticators applies to organizational systems that are accessible to the public (e.g., public-facing websites). External authenticators are issued by nonfederal government entities and are compliant with

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

TAMU-CC shall:

1) Accept only external authenticators that are NIST-compliant; and
2) Document and maintain a list of accepted external authenticators.

IA-8(3) Use of Ficam-approved Products

Withdrawn: Incorporated into IA-8.2

IA-8(4) Use of Defined Profiles

Description

Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the Federal Government assesses and scopes the standards and technology implementations against applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Conform to the following profiles for identity management *[Assignment: identity management profiles]*.

IA-8(5) Acceptance of PIV-I Credentials

Description

Acceptance of PIV-I credentials can be implemented by PIV, PIV-I, and other commercial or external identity providers. The acceptance and verification of PIV-I-compliant credentials apply to both logical and physical access control systems. The acceptance and verification of PIV-I credentials address nonfederal issuers of identity cards that desire to interoperate with United States Government PIV systems and that can be trusted by Federal Government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is commensurate with the PIV credentials as defined in cited references. PIV-I credentials are the credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified with the

FBCA (directly or through another PKI bridge) with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Accept and verify federated or PKI credentials that meet *policy*.

IA-8(6) Disassociability

Description

Federated identity solutions can create increased privacy risks due to the tracking and profiling of individuals. Using identifier mapping tables or cryptographic techniques to blind credential service providers and relying parties from each other or to make identity attributes less visible to transmitting parties can reduce these privacy risks.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: *[Assignment: measures]*.

IA-9 Service Identification and Authentication

Description

Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

Related Controls

IA-3, IA-4, IA-5, SC-8

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Uniquely identify and authenticate *system services and applications* before establishing communications with devices, users, or other services or applications.

IA-9(1) Information Exchange

Withdrawn: Incorporated into IA-9

IA-9(2) Transmission of Decisions

Withdrawn: Incorporated into IA-9

IA-10 Adaptive Authentication

Description

Adversaries may compromise individual authentication mechanisms employed by organizations and subsequently attempt to impersonate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behavior. Suspicious behavior may include accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantities of information than individuals would routinely access; or attempting to access information from suspicious network addresses. When pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information. Another potential use for adaptive authentication is to increase the strength of mechanism based on the number or types of records being accessed. Adaptive authentication does not replace and is not used to avoid the use of multi-factor authentication mechanisms but can augment implementations of multi-factor authentication.

Related Controls

IA-2, IA-8

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Require individuals accessing the system to employ *supplemental authentication techniques or mechanisms* under specific *[Assignment: circumstances or situations]*.

IA-12(1) Supervisor Authorization

Description

Including supervisor or sponsor authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management chain is aware of the account, the account is essential to carry out organizational missions and functions, and the user's privileges are appropriate for the anticipated responsibilities and authorities within the organization.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

IA-12(2) Identity Evidence

Description

Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Require evidence of individual identification be presented to the registration authority.

IA-12(3) Identity Evidence Validation and Verification

Description

Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the users account.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Require that the presented identity evidence be validated and verified through *methods of validation and verification*.

IA-12(4) In-person Validation and Verification

Description

In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

IA-12(5) Address Confirmation

Description

To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

Related Controls

IA-12

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Require that a *registration code or notice of proofing* be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

IA-12(6) Accept Externally-proofed Identities

Description

To limit unnecessary re-proofing of identities, particularly of non-PIV users, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and the identity assurance level appropriate for the system, application, or information accessed. Accepting externally-proofed identities is a fundamental component of managing federated identities across agencies and organizations.

Related Controls

IA-3, IA-4, IA-5, IA-8

Applicability

This Control applies to all TAMU-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation

Accept externally-proofed identities at *[Assignment: identity assurance level]*.

Incident Response – 32 controls

IR-2(1) Simulated Events

Description

Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

Implementation

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

IR-2(2) Automated Training Environments

Description

Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

Implementation

Provide an incident response training environment using *automated mechanisms*.

IR-2(3) Breach

Description

For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes. The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR2(1).

Implementation

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

IR-3(1) Automated Testing

Description

Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities. This can be accomplished by providing more complete coverage of incident response issues, selecting realistic test scenarios and environments, and stressing the response capability.

Implementation

Test the incident response capability using *automated mechanisms*.

IR-3(2) Coordination with Related Plans

Description

Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Implementation

Coordinate incident response testing with organizational elements responsible for related plans.

IR-3(3) Continuous Improvement

Description

To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

Implementation

Use qualitative and quantitative data from testing to: (a) Determine the effectiveness of incident response processes; (b) Continuously improve incident response processes; and (c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

IR-4(1) Automated Incident Handling Processes

Description

Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Implementation

Support the incident handling process using *automated mechanisms*.

IR-4(2) Dynamic Reconfiguration

Description

Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers, and isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include specific time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

Related Controls

AC-2, AC-4, CM-2

Implementation

Include the following types of dynamic reconfiguration for *system components* as part of the incident response capability: *[Assignment: types of dynamic reconfiguration]*.

IR-4(3) Continuity of Operations

Description

Classes of incidents include malfunctions due to design or implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system degradation, system shutdown, fall back to manual mode or activation of alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved for when systems are under attack. Organizations consider whether continuity of operations requirements during an incident conflict with the capability to automatically disable the system as specified as part of IR-4(5).

Implementation

Identify *classes of incidents* and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: *[Assignment: actions]*.

IR-4(4) Information Correlation

Description

Sometimes, a threat event, such as a hostile cyber-attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Implementation

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

IR-4(5) Automatic Disabling of System

Description

Organizations consider whether the capability to automatically disable the system conflicts with continuity of operations requirements specified as part of CP-2 or IR-4(3) . Security violations include cyber-attacks that have compromised the integrity of the system or exfiltrated organizational information and serious errors in software programs that could adversely impact organizational missions or functions or jeopardize the safety of individuals.

Implementation

Implement a configurable capability to automatically disable the system if *security violations* are detected.

IR-4(6) Insider Threats

Description

Explicit focus on handling incidents involving insider threats provides additional emphasis on this type of threat and the need for specific incident handling capabilities to provide appropriate and timely responses.

Implementation

Implement an incident handling capability for incidents involving insider threats.

IR-4(7) Insider Threats - Intra-organization Coordination

Description

Incident handling for insider threat incidents (e.g., preparation, detection and analysis, containment, eradication, and recovery) requires coordination among many organizational entities, including

mission or business owners, system owners, human resources offices, procurement offices, personnel offices, physical security offices, senior agency information security officer, operations personnel, risk executive (function), senior agency official for privacy, and legal counsel. In addition, organizations may require external support from federal, state, and local law enforcement agencies.

Implementation

Coordinate an incident handling capability for insider threats that includes the following organizational entities:

1) Texas DIR;
2) TAMUS SOC; and
3) TAMUS CRT.

IR-4(8) Correlation with External Organizations

Description

The coordination of incident information with external organizations-including mission or business partners, military or coalition partners, customers, and developers-can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and breaches that could potentially affect the organization’s operations, assets, and individuals.

Related Controls

AU-16, PM-16

Implementation

Coordinate with *external organizations* to correlate and share *incident information* to achieve a cross-organization perspective on incident awareness and more effective incident responses.

IR-4(9) Dynamic Response Capability

Description

The dynamic response capability addresses the timely deployment of new or replacement organizational capabilities in response to incidents. This includes capabilities implemented at the mission and business process level and at the system level.

Implementation

Employ *dynamic response capabilities* to respond to incidents.

IR-4(10) Supply Chain Coordination

Description

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents can occur anywhere through or to the supply chain and include compromises or breaches that involve primary or sub-tier providers, information technology products, system components, development processes or personnel, and distribution processes or warehousing facilities. Organizations consider including processes for protecting and sharing incident information in information exchange agreements and their obligations for reporting incidents to government oversight bodies (e.g., Federal Acquisition Security Council).

Related Controls

CA-3, MA-2, SA-9, SR-8

Implementation

Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

IR-4(11) Integrated Incident Response Team

Description

An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security and privacy engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity. An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the
development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development. Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

Related Controls

AT-3

Implementation

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in *four (4) hours*.

IR-4(12) Malicious Code and Forensic Analysis

Description

When conducted carefully in an isolated environment, analysis of malicious code and other residual artifacts of a security incident or breach can give the organization insight into adversary tactics, techniques, and procedures. It can also indicate the identity or some defining characteristics of the adversary. In addition, malicious code analysis can help the organization develop responses to future incidents.

Implementation

Analyze malicious code and/or other residual artifacts remaining in the system after the incident.

IR-4(13) Behavior Analysis

Description

If the organization maintains a deception environment, an analysis of behaviors in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial tactics, techniques, and procedures. External to a deception environment, the analysis of anomalous adversarial behavior (e.g., changes in system performance or usage patterns) or suspected behavior (e.g., changes in searches for the location of specific resources) can give the organization such insight.

Implementation

Analyze anomalous or suspected adversarial behavior in or related to *environments or resources*.

IR-4(14) Security Operations Center

Description

A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and securityrelevant event data from multiple sources. These sources include perimeter defenses, network devices (e.g., routers, switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ thirdparty organizations to provide such a capability.

Implementation

Establish and maintain a security operations center.

IR-4(15) Public Relations and Reputation Repair

Description

It is important for an organization to have a strategy in place for addressing incidents that have been brought to the attention of the general public, have cast the organization in a negative light, or have affected the organization's constituents (e.g., partners, customers). Such publicity can be extremely harmful to the organization and affect its ability to carry out its mission and business functions. Taking proactive steps to repair the organization's reputation is an essential aspect of reestablishing the trust and confidence of its constituents.

Implementation

TAMU-CC shall:

1) Manage public relations associated with an incident; and
2) Employ measures to repair the reputation of the organization.

IR-5(1) Automated Tracking, Data Collection, and Analysis

Description

Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

Implementation

Track incidents and collect and analyze incident information using *automated mechanisms*.

IR-6(1) Automated Reporting

Description

The recipients of incident reports are specified in

Related Controls

IR-7

Implementation

Report incidents using *automated mechanisms*.

IR-6(2) Vulnerabilities Related to Incidents

Description

Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.

Implementation

Report system vulnerabilities associated with reported incidents to *the Office of Information Security*.

IR-6(3) Supply Chain Coordination

Description

Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include the Federal Acquisition Security Council (FASC). Supply chain incidents include compromises or breaches that involve information technology products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations determine the appropriate information to share and consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related Controls

SR-8

Implementation

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

IR-7(1) Automation Support for Availability of Information and Support

Description

Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Implementation

Increase the availability of incident response information and support using *automated mechanisms*.

IR-7(2) Coordination with External Providers

Description

External providers of a system protection capability include the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks. It may be beneficial to have agreements in place with external providers to clarify the roles and responsibilities of each party before an incident occurs.

Implementation

TAMU-CC shall:

1) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and
2) Identify organizational incident response team members to the external providers.

IR-8(1) Breaches

Description

Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, including notice to individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements.

Related Controls

PT-1, PT-2, PT-3, PT-4, PT-5, PT-7

Implementation

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

1) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
2) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
3) Identification of applicable privacy requirements.

IR-9(1) Responsible Personnel

Withdrawn: Incorporated into IR-9

IR-9(2) Training

Description

Organizations establish requirements for responding to information spillage incidents in incident response plans. Incident response training on a regular basis helps to ensure that organizational personnel understand their individual responsibilities and what specific actions to take when spillage incidents occur.

Related Controls

AT-2, AT-3, CP-3, IR-2

Implementation

Provide information spillage response training *annually*.

IR-9(3) Post-spill Operations

Description

Corrective actions for systems contaminated due to information spillages may be timeconsuming. Personnel may not have access to the contaminated systems while corrective actions are being taken, which may potentially affect their ability to conduct organizational business.

Implementation

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: *[Assignment: procedures]*.

IR-9(4) Exposure to Unauthorized Personnel

Description

Controls include ensuring that personnel who are exposed to spilled information are made aware of the laws, executive orders, directives, regulations, policies, standards, and guidelines regarding the information and the restrictions imposed based on exposure to such information.

Implementation

Employ the following controls for personnel exposed to information not within assigned access authorizations: *[Assignment: controls]*.

IR-10 Integrated Information Security Analysis Team

Withdrawn: Moved to IR-4.11

Maintenance – 24 controls

MA-2(1) Record Content

Withdrawn: Incorporated into MA-2

MA-2(2) Automated Maintenance Activities

Description

The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

Related Controls

MA-3

Implementation

TAMU-CC shall

1) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using *automated mechanisms* ; and
2) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

MA-3 Maintenance Tools

Description

Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers. The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as

Related Controls

MA-2, PE-16

References

SP 800-88

Implementation

TAMU-CC shall:

1) Approve, control, and monitor the use of system maintenance tools; and

2) Review previously approved system maintenance tools *annually*.

MA-3(1) Inspect Tools

Description

Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related Controls

SI-7

Implementation

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

MA-3(2) Inspect Media

Description

If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related Controls

SI-3

Implementation

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

MA-3(3) Prevent Unauthorized Removal

Description

Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related Controls

MP-6

Implementation

Prevent the removal of maintenance equipment containing organizational information by:

1) Verifying that there is no organizational information contained on the equipment;
2) Sanitizing or destroying the equipment;

3) Retaining the equipment within the facility; or
4) Obtaining an exemption from *the Office of Information Security* explicitly authorizing removal of the equipment from the facility.

MA-3(4) Restricted Tool Use

Description

Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.

Related Controls

AC-3, AC-5, AC-6

Implementation

Restrict the use of maintenance tools to authorized personnel only.

MA-3(5) Execution with Privilege

Description

Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.

Related Controls

AC-3, AC-6

Implementation

Monitor the use of maintenance tools that execute with increased privilege.

MA-3(6) Software Updates and Patches

Description

Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.

Related Controls

AC-3, AC-6

Implementation

Inspect maintenance tools to ensure the latest software updates and patches are installed.

MA-4(1) Logging and Review

Description

Audit logging for nonlocal maintenance is enforced by AU-2 . Audit events are defined in

Related Controls

AU-6, AU-12

Implementation

TAMU-CC shall:

1) Log *audit events* for nonlocal maintenance and diagnostic sessions; and
2) Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

MA-4(2) Document Nonlocal Maintenance

Withdrawn: Incorporated into MA-1, MA-4

MA-4(3) Comparable Security and Sanitization

Description

Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related Controls

MP-6, SI-3, SI-7

Implementation

TAMU-CC shall:

1) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
2) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

MA-4(4) Authentication and Separation of Maintenance Sessions

Description

Communications paths can be logically separated using encryption.

Implementation

Protect nonlocal maintenance sessions by:

1) Employing *authenticators that are replay resistant*; and
2) Separating the maintenance sessions from other network sessions with the system by either:
    a. Physically separated communications paths; or
    b. Logically separated communications paths.

MA-4(5) Approvals and Notifications

Description

Notification may be performed by maintenance personnel. Approval of nonlocal maintenance is accomplished by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Implementation

TAMU-CC shall:

1) Require the approval of each nonlocal maintenance session by *the Change Advisory Board*; and
2) Notify the following personnel or roles of the date and time of planned nonlocal maintenance:
    a. Student
    b. Staff
    c. Faculty

MA-4(6) Cryptographic Protection

Description

Failure to protect nonlocal maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized access during remote maintenance sessions can result in a variety of hostile actions, including malicious code insertion,

unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.

Related Controls

SC-8, SC-12, SC-13

Implementation

Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: *[Assignment: cryptographic mechanisms]*.

MA-4(7) Disconnect Verification

Description

Verifying the termination of a connection once maintenance is completed ensures that connections established during nonlocal maintenance and diagnostic sessions have been terminated and are no longer available for use.

Related Controls

AC-12

Implementation

Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

MA-5(1) Individuals Without Appropriate Access

Description

Procedures for individuals who lack appropriate security clearances or who are not U.S. citizens are intended to deny visual and electronic access to classified or controlled unclassified information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Related Controls

MP-6, PL-2

Implementation

TAMU-CC shall:

1) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
    a. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
    b. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2) Develop and implement *alternate controls* in the event a system component cannot be sanitized, removed, or disconnected from the system.

MA-5(2) Security Clearances for Classified Systems

Description

Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. To mitigate the inherent risk of such exposure, organizations use maintenance personnel that are cleared (i.e., possess security clearances) to the classification level of the information stored on the system.

Related Controls

PS-3

Implementation

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.

MA-5(3) Citizenship Requirements for Classified Systems

Description

Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. If access to classified information on organizational systems is restricted to U.S. citizens, the same restriction is applied to personnel performing maintenance on those systems.

Related Controls

PS-3

Implementation

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.

MA-5(4) Foreign Nationals

Description

Personnel who conduct maintenance and diagnostic activities on organizational systems may be exposed to classified information. If non-U.S. citizens are permitted to perform maintenance and diagnostics activities on classified systems, then additional vetting is required to ensure agreements and restrictions are not being violated.

Related Controls

PS-3

Implementation

TAMU-CC shall ensure that:

1) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and
2) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

MA-5(5) Non-system Maintenance

Description

Personnel who perform maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.

Implementation

Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

MA-6 Timely Maintenance

Description

Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related Controls

CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4

Implementation

Obtain maintenance support and/or spare parts for *system components* within *twenty-four (24)* of failure.

MA-6(1) Preventive Maintenance

Description

Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid or mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they fail. Methods of determining what preventive (or other) failure management policies to apply include original equipment manufacturer recommendations; statistical failure records; expert opinion; maintenance that has already been conducted on similar equipment; requirements of codes, laws, or regulations within a jurisdiction; or measured values and performance indications.

Implementation

Perform preventive maintenance on *system components* at *regular time intervals*.

MA-6(2) Predictive Maintenance

Description

Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the objective of predicting the future trend of the equipment’s condition. The predictive maintenance approach employs principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thus minimizing disruption of normal

system operations. Predictive maintenance can result in substantial cost savings and higher system reliability.

Implementation

Perform predictive maintenance on *system components* at *regular time intervals*.

MA-6(3) Automated Support for Predictive Maintenance

Description

A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates the processing of equipment condition data to trigger maintenance planning, execution, and reporting.

Implementation

Transfer predictive maintenance data to a maintenance management system using *automated mechanisms*.

MA-7 Field Maintenance

Description

Field maintenance is the type of maintenance conducted on a system or system component after the system or component has been deployed to a specific site (i.e., operational environment). In certain instances, field maintenance (i.e., local maintenance at the site) may not be executed with the same degree of rigor or with the same quality control checks as depot maintenance. For critical systems designated as such by the organization, it may be necessary to restrict or prohibit field maintenance at the local site and require that such maintenance be conducted in trusted facilities with additional controls.

Related Controls

MA-2, MA-4, MA-5

Implementation

Restrict or prohibit field maintenance on *systems or system components* to *trusted maintenance facilities*.

Media Protection – 15 controls

MP-4 Media Storage

Description

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related Controls

AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12

Implementation

TAMU-CC shall:

1) Physically control and securely store *types of digital and/or non-digital media* within *controlled areas* ; and

2) Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

References

FIPS 199, SP 800-56A, SP 800-56B, SP 800-56C, SP 800-57-1, SP 800-57-2, SP 800-57-3, SP 800-111

MP-4(1) Cryptographic Protection

Withdrawn: Incorporated into SC-28.1

MP-4(2) Automated Restricted Access

Description

Automated mechanisms include keypads, biometric readers, or card readers on the external entries to media storage areas.

Related Controls

AC-3, AU-2, AU-6, AU-9, AU-12, PE-3

Implementation

Restrict access to media storage areas and log access attempts and access granted using *automated mechanisms]*.

MP-5 Media Transport

Description

System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related Controls

AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34

References

FIPS 199, SP 800-60-1, SP 800-60-2

Implementation

TAMU-CC shall:

1) Protect and control *system media* during transport outside of controlled areas using security *controls*;

2) Maintain accountability for system media during transport outside of controlled areas;

3) Document activities associated with the transport of system media; and

4) Restrict the activities associated with the transport of system media to authorized personnel.

MP-5(1) Protection Outside of Controlled Areas

Withdrawn: Incorporated into MP-5

MP-5(2) Documentation of Activities

Withdrawn: Incorporated into MP-5

MP-5(3) Custodians

Description

Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified.

Implementation

Employ an identified custodian during transport of system media outside of controlled areas.

MP-5(4) Cryptographic Protection

Withdrawn: Incorporated into SC-28.1

MP-6(1) Review, Approve, Track, Document, and Verify

Description

Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations verify that the sanitization of the media was effective prior to disposal.

Implementation

Review, approve, track, document, and verify media sanitization and disposal actions.

MP-6(2) Equipment Testing

Description

Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal agencies or external service providers.

Implementation

Test sanitization equipment and procedures *annually* to ensure that the intended sanitization is being achieved.

MP-6(3) Nondestructive Techniques

Description

Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals. While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations consider nondestructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

MP-6(4) Controlled Unclassified Information

Withdrawn: Incorporated into MP-6

MP-6(5) Classified Information

Withdrawn: Incorporated into MP-6

MP-6(6) Media Destruction

Withdrawn: Incorporated into MP-6

Implementation

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: *[Assignment: circumstances]*.

MP-6(7) Dual Authorization

Description

Organizations employ dual authorization to help ensure that system media sanitization cannot occur unless two technically qualified individuals conduct the designated task. Individuals who sanitize system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related Controls

AC-3, MP-2

Implementation

Enforce dual authorization for the sanitization of *[Assignment: system media]*.

MP-6(8) Remote Purging or Wiping of Information

Implementation

Provide the capability to purge or wipe information from *systems or system components remotely.*

Description

Remote purging or wiping of information protects information on organizational systems and system components if systems or components are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the system, component, or device. The purge or wipe function can be

implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted data.

MP-7(1) Prohibit Use Without Owner

Withdrawn: Incorporated into MP-7

MP-7(2) Prohibit Use of Sanitization-resistant Media

Description

Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media. Certain types of media do not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

Related Controls

MP-6

Implementation

Prohibit the use of sanitization-resistant media in organizational systems.

MP-8 Media Downgrading

Description

Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process removes information from the media, typically by security category or

classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading ensures that empty space on the media is devoid of information.

References

32 CFR 2002, NSA MEDIA

Implementation

TAMU-CC shall:

1) Establish *system media downgrading process* that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;

2) Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

3) Identify *system media requiring downgrading* ; and

4) Downgrade the identified system media using the established process.

MP-8(1) Documentation of Process

Description

Organizations can document the media downgrading process by providing information, such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

Implementation

Document system media downgrading actions.

MP-8(2) Equipment Testing

Description

None.

Implementation

Test downgrading equipment and procedures *[Assignment: organization-defined frequency]* to ensure that downgrading actions are being achieved.

MP-8(3) Controlled Unclassified Information

Description

The downgrading of controlled unclassified information uses approved sanitization tools, techniques, and procedures.

Implementation

Downgrade system media containing controlled unclassified information prior to public release.

MP-8(4) Classified Information

Description

Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.

Implementation

Downgrade system media containing classified information prior to release to individuals without required access authorizations.

Physical and Environmental Protection – 40 controls

PE-2(1) Access by Position or Role

Description

Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.

Related Controls

AC-2, AC-3, AC-6

Implementation

Authorize physical access to the facility where the system resides based on position or role.

PE-2(2) Two Forms of Identification

Description

Acceptable forms of identification include passports, REAL ID-compliant drivers' licenses, and Personal Identity Verification (PIV) cards. For gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics.

Related Controls

IA-2, IA-4, IA-5

Implementation

Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: *[Assignment: list of acceptable forms of identification]*.

PE-2(3) Restrict Unescorted Access

Description

Individuals without required security clearances, access approvals, or need to know are escorted by individuals with appropriate physical access authorizations to ensure that information is not exposed or otherwise compromised.

Related Controls

PS-2, PS-6

Implementation

Restrict unescorted access to the facility where the system resides to personnel with *security clearances for all information contained within the system, formal access authorizations for all information contained within the system, or need for access to all information contained within the system*.

PE-3(1) System Access

Description

Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Implementation

Enforce physical access authorizations to the system in addition to the physical access controls for the facility *physical spaces*.

PE-3(2) Facility and Systems

Description

Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Related Controls

AC-4, SC-7

Implementation

Perform security checks *quarterly* at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

PE-3(3) Continuous Guards

Description

Employing guards at selected physical access points to the facility provides a more rapid response capability for organizations. Guards also provide the opportunity for human surveillance in areas of the facility not covered by video surveillance.

Related Controls

CP-6, CP-7, PE-6

Implementation

Employ guards to control *physical access points* to the facility where the system resides 24 hours per day, 7 days per week.

PE-3(4) Lockable Casings

Description

The greatest risk from the use of portable devices-such as smart phones, tablets, and notebook computers-is theft. Organizations can employ lockable, physical casings to reduce or eliminate the risk of equipment theft. Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals. Lockable physical casings can be used in conjunction with cable locks or lockdown plates to prevent the theft of the locked casing containing the computer equipment.

Implementation

Use lockable physical casings to protect *[Assignment: system components]* from unauthorized physical access.

PE-3(5) Tamper Protection

Description

Organizations can implement tamper detection and prevention at selected hardware components or implement tamper detection at some components and tamper prevention at other components. Detection and prevention activities can employ many types of anti-tamper technologies, including tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

Related Controls

SA-16, SR-9, SR-11

PE-3(6) Facility Penetration Testing

Withdrawn: Incorporated into CA-8

Implementation

Employ *anti-tamper technologies* to *detect or prevent* physical tampering or alteration of *hardware components* within the system.

PE-3(7) Physical Barriers

Description

Physical barriers include bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.

Implementation

Limit access using physical barriers.

PE-3(8) Access Control Vestibules

Description

An access control vestibule is part of a physical access control system that typically provides a space between two sets of interlocking doors. Vestibules are designed to prevent unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as piggybacking or tailgating, results in unauthorized access to the facility. Interlocking door controllers can be used to limit the number of individuals who enter controlled access points and to provide containment areas while authorization for physical access is verified. Interlocking door controllers can be fully automated (i.e., controlling the opening and closing of the doors) or partially automated (i.e., using security guards to control the number of individuals entering the containment area).

Implementation

Employ access control vestibules at areas *storing controlled or confidential information systems*.

PE-4 Access Control for Transmission

Description

Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related Controls

AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8

Implementation

Control physical access to *system distribution and transmission lines* within organizational facilities using *security controls*.

PE-5 Access Control for Output Devices

Description

Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing

monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related Controls

PE-2, PE-3, PE-4, PE-18

Implementation

Control physical access to output from *output devices* to prevent unauthorized individuals from obtaining the output.

PE-5(1) Access to Output by Authorized Individuals

Withdrawn: Incorporated into PE-5

PE-5(2) Link to Individual Identity

Description

Methods for linking individual identity to the receipt of output from output devices include installing security functionality on facsimile machines, copiers, and printers. Such functionality allows organizations to implement authentication on output devices prior to the release of output to individuals.

Implementation

Link individual identity to receipt of output from output devices.

PE-5(3) Marking Output Devices

Withdrawn: Incorporated into PE-22

PE-6(1) Intrusion Alarms and Surveillance Equipment

Description

Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached. Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility.

Implementation

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

PE-6(2) Automated Intrusion Recognition and Responses

Description

Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email and text messages, and activating door locking mechanisms. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide integrated threat coverage for the organization.

Related Controls

SI-4

Implementation

Recognize *intrusions* and initiate *response actions* using *automated mechanisms*.

PE-6(3) Video Surveillance

Description

Video surveillance focuses on recording activity in specified areas for the purposes of subsequent review, if circumstances so warrant. Video recordings are typically reviewed to detect anomalous events or incidents. Monitoring the surveillance video is not required, although organizations may choose to do so. There may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location.

Implementation

TAMU-CC shall:

1) Employ video surveillance of *operational areas*;
2) Review video recordings monthly ; and
3) Retain video recordings for *one (1) year.*

PE-6(4) Monitoring Physical Access to Systems

Description

Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centers. Physical access monitoring can be coordinated with intrusion

detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Implementation

Monitor physical access to the system in addition to the physical access monitoring of the facility at *physical spaces that contain controlled or confidential information*.

PE-7 Visitor Control

Withdrawn: Incorporated into PE-2, PE-3

PE-8(1) Automated Records Maintenance and Review

Description

Visitor access records may be stored and maintained in a database management system that is accessible by organizational personnel. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions.

Implementation

Maintain and review visitor access records using *automated mechanisms*.

PE-8(2) Physical Access Records

Withdrawn: Incorporated into PE-2

PE-8(3) Limit Personally Identifiable Information Elements

Description

Organizations may have requirements that specify the contents of visitor access records. Limiting personally identifiable information in visitor access records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls

RA-3, SA-8

Implementation

Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment:

1) Name
2) Date of visit
3) Reason for visit

PE-9 Power Equipment and Cabling

Implementation

Protect power equipment and power cabling for the system from damage and destruction.

Description

Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptable power sources in offices or data centers, generators and power cabling outside of

buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related Controls

PE-4

PE-9(1) Redundant Cabling

Description

Physically separate and redundant power cables ensure that power continues to flow in the event that one of the cables is cut or otherwise damaged.

Implementation

Employ redundant power cabling paths that are physically separated by *one (1) foot.*

PE-9(2) Automatic Voltage Controls

Description

Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.

Implementation

Employ automatic voltage controls for *critical system components*.

PE-10 Emergency Shutoff

Description

Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related Controls

PE-15

Implementation

TAMU-CC shall:

1) Provide the capability of shutting off power to *system or individual system components* in emergency situations;

2) Place emergency shutoff switches or devices in *the data operation center* to facilitate access for authorized personnel; and

3) Protect emergency power shutoff capability from unauthorized activation.

PE-10(1) Accidental and Unauthorized Activation

Withdrawn: Incorporated into PE-10

PE-11 Emergency Power

Description

An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centers, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or properly shut down the system.

Related Controls

AT-3, CP-2, CP-7

Implementation

Provide an uninterruptible power supply to facilitate *an orderly shutdown of the system and transition of the systems to long-term alternate power* in the event of a primary power source loss.

PE-11(1) Alternate Power Supply - Minimal Operational Capability

Description

Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Implementation

Provide an alternate power supply for the system that is activated *manually or automatically* and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

PE-11(2) Alternate Power Supply - Self-contained

Description

The provision of a long-term, self-contained power supply can be satisfied by using one or more generators with sufficient capacity to meet the needs of the organization.

Implementation

Provide an alternate power supply for the system that is activated *manually or automatically* and that is:

1) Self-contained;
2) Not reliant on external power generation; and
3) Capable of maintaining *minimally required operational capability* in the event of an extended loss of the primary power source.

PE-12(1) Essential Mission and Business Functions

Description

Organizations define their essential missions and functions.

Implementation

Provide emergency lighting for all areas within the facility supporting essential mission and business functions.

PE-13(1) Detection Systems - Automatic Activation and Notification

Description

Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Implementation

Employ fire detection systems that activate automatically and notify University Police Department and *emergency responders* in the event of a fire.

PE-13(2) Suppression Systems - Automatic Activation and Notification

Description

Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

PE-13(3) Automatic Fire Suppression

Withdrawn: Incorporated into PE-13.2

Implementation

TAMU-CC shall:

1) Employ fire suppression systems that activate automatically and notify *University Police Department* and *emergency responders;* and
2) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

PE-13(4) Inspections

Description

Authorized and qualified personnel within the jurisdiction of the organization include state, county, and city fire inspectors and fire marshals. Organizations provide escorts during inspections in situations where the systems that reside within the facilities contain sensitive information.

Implementation

Ensure that the facility undergoes annual fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within ninety (90) days.

PE-14(1) Automatic Controls

Description

The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.

Implementation

Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: *[Assignment: automatic environmental controls]*.

PE-14(2) Monitoring with Alarms and Notifications

Description

The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

Implementation

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to *Networking Staff and University Police Department*.

PE-15(1) Automation Support

Description

Automated mechanisms include notification systems, water detection sensors, and alarms.

Implementation

Detect the presence of water near the system and alert *Networking staff and University Police Department* using *automated mechanisms*.

PE-18 Location of System Components

Description

Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity

can increase the risk of unauthorized access to organizational communications using wireless packet sniffers or microphones, or unauthorized disclosure of information.

Related Controls

CP-2, PE-5, PE-19, PE-20, RA-3

Implementation

Position system components within the facility to minimize potential damage from *physical and environmental hazards* and to minimize the opportunity for unauthorized access.

PE-18(1) Facility Site

Withdrawn: Moved to PE-23

PE-19 Information Leakage

Description

Information leakage is the intentional or unintentional release of data or information to an untrusted environment from electromagnetic signals emanations. The security categories or classifications of systems (with respect to confidentiality), organizational security policies, and risk tolerance guide the selection of controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Related Controls

AC-18, PE-18, PE-20

Implementation

Protect the system from information leakage due to electromagnetic signals emanations.

PE-19(1) National Emissions Policies and Procedures

Description

Emissions Security (EMSEC) policies include the former TEMPEST policies.

Implementation

Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.

PE-20 Asset Monitoring and Tracking

Description

Asset location technologies can help ensure that critical assets-including vehicles, equipment, and system components-remain in authorized locations. Organizations consult with the Office of the General Counsel and senior agency official for privacy regarding the deployment and use of asset location technologies to address potential privacy concerns.

Related Controls

CM-8, PE-16, PM-8

Implementation

Employ *asset location technologies* to track and monitor the location and movement of *assets* within *controlled areas*.

PE-21 Electromagnetic Pulse Protection

Description

An electromagnetic pulse (EMP) is a short burst of electromagnetic energy that is spread over a range of frequencies. Such energy bursts may be natural or man-made. EMP interference may be disruptive or damaging to electronic equipment. Protective measures used to mitigate EMP risk include shielding, surge suppressors, ferro-resonant transformers, and earth grounding. EMP protection may be especially significant for systems and applications that are part of the U.S. critical infrastructure.

Related Controls

PE-18, PE-19

Implementation

Employ *protective measures* against electromagnetic pulse damage for *system and system components*.

PE-22 Component Marking

Description

Hardware components that may require marking include input and output devices. Input devices include desktop and notebook computers, keyboards, tablets, and smart phones. Output devices

include printers, monitors/video displays, facsimile machines, scanners, copiers, and audio devices. Permissions controlling output to the output devices are addressed in AC-3 or AC-4 . Components are marked to indicate the impact level or classification level of the system to which the devices are connected, or the impact level or classification level of the information permitted to be output. Security marking refers to the use of human-readable security attributes. Security labeling refers to the use of security attributes for internal system data structures. Security marking is generally not required for hardware components that process, store, or transmit information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components that process, store, or transmit public information in order to indicate that such information is publicly releasable. Marking of system hardware components reflects applicable laws, executive orders, directives, policies, regulations, and standards.

Related Controls

AC-3, AC-4, AC-16, MP-3

Implementation

Mark *system hardware components* indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

PE-23 Facility Location

Description

Physical and environmental hazards include floods, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. The location of system components within the facility is addressed in PE-18.

Related Controls

CP-2, PE-18, PE-19, PM-8, PM-9, RA-3

Implementation

TAMU-CC shall:

1) Plan the location or site of the facility where the system resides considering physical and environmental hazards; and

2) For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

Planning – 8 controls

PL-2(1) Concept of Operations

Withdrawn: Incorporated into PL-7

PL-2(2) Functional Architecture

Withdrawn: Incorporated into PL-8

PL-2(3) Plan and Coordinate with Other Organizational Entities

Withdrawn: Incorporated into PL-2

PL-3 System Security Plan Update

Withdrawn: Incorporated into PL-2

PL-4(1) Social Media and External Site/application Usage Restrictions

Description

Social media, social networking, and external site/application usage restrictions address rules of behavior related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personally identifiable information and system account information.

Related Controls

AC-22, AU-13

Implementation

Include in the rules of behavior, restrictions on:

1) Use of social media, social networking sites, and external sites/applications;
2) Posting organizational information on public websites; and
3) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

PL-5 Privacy Impact Assessment

Withdrawn: Incorporated into RA-8

PL-6 Security-related Activity Planning

Withdrawn: Incorporated into PL-2

PL-7 Concept of Operations

Description

The CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents. The CONOPS is a living document that requires updating throughout the system development life cycle. For example, during system design reviews, the concept of operations is checked to ensure that it remains consistent with the design for controls, the system architecture, and the operational procedures. Changes to the CONOPS are reflected in ongoing updates to the security and privacy plans, security and privacy architectures, and other organizational documents, such as procurement specifications, system development life cycle documents, and systems engineering documents.

Related Controls

PL-2, SA-2, SI-12

Implementation

TAMU-CC shall:

a. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and

b. Review and update the CONOPS *annualy*.

PL-8 Security and Privacy Architectures

Description

The security and privacy architectures at the system level are consistent with the organizationwide security and privacy architectures described in PM-7 , which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures. PL-8 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external information technology product and system developers and integrators. SA-17 , which is complementary to PL-8 , is selected when organizations outsource the development of systems or

components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Related Controls

CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7

Implementation

TAMU-CC shall:

1) Develop security and privacy architectures for the system that:

    a) Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

    b) Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

    c) Describe how the architectures are integrated into and support the enterprise architecture; and

    d) Describe any assumptions about, and dependencies on, external systems and services;

2) Review and update the architectures *annually* to reflect changes in the enterprise architecture; and

3) Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-8(1) Defense in Depth

Description

Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering.

Defense-in-depth architectural approaches include modularity and layering (see SA-8(3)), separation of system and user functionality (see SC-2), and security function isolation (see SC3).

Related Controls

SC-2, SC-3, SC-29, SC-36

Implementation

Design the security and privacy architectures for the system using a defense-in-depth approach that:

1) Allocates *controls* to *locations and architectural layers*; and
2) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

PL-8(2) Supplier Diversity

Description

Information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious

code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By deploying different products at different locations, there is an increased likelihood that at least one of the products will detect the malicious code. With respect to privacy, vendors may offer products that track personally identifiable information in systems. Products may use different tracking methods. Using multiple products may result in more assurance that personally identifiable information is inventoried.

Related Controls

SC-29, SR-3

Implementation

Require that *controls* allocated to *locations and architectural layers* are obtained from different suppliers.

PL-9 Central Management

Description

Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring. Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities; alerting mechanisms; and dashboards to support risk-

based decision-making within the organization. As part of the control selection processes, organizations determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-2(1), AC-2(2), AC-2(3), AC-2(4),

Related Controls

PL-8, PM-9

Implementation

Centrally manage *controls and related processes*.

PL-10 Baseline Selection

Description

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Federal control baselines are provided in

Related Controls

PL-2, PL-11, RA-2, RA-3, SA-8

Implementation

Select a control baseline for the system.

PL-11 Baseline Tailoring

Description

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in [SP 800-53B] can be supplemented with additional actions based on the needs of organizations. Tailoring actions can be applied to the baselines in [SP 800-53B] in accordance with the security and privacy requirements from [FISMA], [PRIVACT], and [OMB A-130]. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in [SP 800-53B] to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related Controls

PL-10, RA-2, RA-3, RA-9, SA-8

Implementation

Tailor the selected control baseline by applying specified tailoring actions.

Program Management – 24 controls

PM-5(1) Inventory of Personally Identifiable Information

Description

An inventory of systems, applications, and projects that process personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. Organizations may use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein.

Related Controls

AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18

Implementation

Establish, maintain, and update *[Assignment: frequency]* an inventory of all systems, applications, and projects that process personally identifiable information.

PM-8 Critical Infrastructure Plan

Description

Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Related Controls

CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12

Implementation

Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

PM-11 Mission and Business Process Definition

Description

Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and the Nation through the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personally identifiable information processing needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy. Information protection and personally identifiable information processing needs determine the required controls for the organization and the systems. Inherent to defining protection and personally identifiable information processing needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations. Privacy risks to individuals can arise from the compromise of personally identifiable information, but they can also arise as unintended consequences or a byproduct of the processing of personally identifiable information at any stage of the information life cycle. Privacy risk assessments are used to prioritize the risks that are created for individuals from system processing of personally identifiable information. These risk assessments enable the selection of the required privacy controls for the organization and systems. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

Related Controls

CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2

References

OMB A-130, FIPS 199, SP 800-39, SP 800-60-1, SP 800-60-2, SP 800-160-1

Implementation

a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and

c. Review and revise the mission and business processes *[Assignment: frequency]*.

PM-12 Insider Threat Program

Description

Organizations that handle classified information are required, under Executive Order 13587 Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace, including ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts. However, the use of human resource records could raise significant concerns for privacy. The participation of a legal team, including consultation with the senior agency official for privacy, ensures that

monitoring activities are performed in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls

AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14

References

EO 13587, NITP12, ODNI NITP

Implementation

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

PM-13 Security and Privacy Workforce

Description

Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility. The programs encourage organizations to fill security- and privacyrelated positions with qualified personnel. Security and privacy workforce development and improvement programs are

complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals.

Related Controls

AT-2, AT-3

Implementation

Establish a security and privacy workforce development and improvement program.

PM-16(1) Automated Means for Sharing Threat Intelligence

Description

To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

Implementation

Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

PM-17 Protecting Controlled Unclassified Information on External Systems

Description

Controlled unclassified information is defined by the National Archives and Records Administration along with the safeguarding and dissemination requirements for such information and is codified in

Related Controls

CA-6, PM-10

Implementation

a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and

b. Review and update the policy and procedures *[Assignment: organization-defined frequency]*.

PM-18 Privacy Program Plan

Description

A privacy program plan is a formal document that provides an overview of an organization’s privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or

compilations of documents. The senior agency official for privacy is responsible for designating which privacy controls the organization will treat as program management, common, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection operations explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended. Program management controls are generally implemented at the organization level and are essential for managing the organization's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. Together, the privacy plans for individual systems and the organization-wide privacy program plan provide complete coverage for the privacy controls employed within the organization. Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

Related Controls

PM-8, PM-9, PM-19

Implementation

a. Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:

    1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and

b. Update the plan *[Assignment: frequency]* and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

PM-19 Privacy Program Leadership Role

Description

The privacy officer is an organizational official. For federal agencies-as defined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines-this official is designated as the senior agency official for privacy. Organizations may also refer to this official as the chief privacy officer. The senior agency official for privacy also has roles on the data management board (see PM-23) and the data integrity board (see PM-24).

Related Controls

PM-18, PM-20, PM-23, PM-24, PM-27

Implementation

Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

PM-20 Dissemination of Privacy Program Information

Description

For federal agencies, the webpage is located at www.[agency].gov/privacy. Federal agencies include public privacy impact assessments, system of records notices, computer matching notices and agreements, {#18e71fec-c6fd-475a-925a-5d8495cf8455} exemption and implementation rules, privacy reports, privacy policies, instructions for individuals making an access or amendment request, email addresses for questions/complaints, blogs, and periodic publications.

Related Controls

AC-3, PM-19, PT-5, PT-6, PT-7, RA-8

Implementation

Maintain a central resource webpage on the organization’s principal public website that serves as a central source of information about the organization’s privacy program and that: a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b. Ensures that organizational privacy practices and reports are publicly available; and c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

PM-20(1) Privacy Policies on Websites, Applications, and Digital Services

Description

Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. In addition, organizations provide a link to the privacy policy on any webpage that collects personally identifiable information. Organizations may be subject to applicable laws, executive orders, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Implementation

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: (a) Are written in plain language and organized in a way that is easy to understand and navigate; (b) Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and (c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

PM-21 Accounting of Disclosures

Description

The purpose of accounting of disclosures is to allow individuals to learn to whom their personally identifiable information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or disputed personally identifiable information, and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures. For federal agencies, keeping an accounting of disclosures is required by the {#18e71fec-c6fd-475a925a-5d8495cf8455} ; agencies should consult with their senior agency official for privacy and legal

counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision. Organizations can use any system for keeping notations of disclosures, if it can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personally identifiable information is disclosed, including commercial services that provide notifications and alerts. Accounting of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

Related Controls

AC-3, AU-2, PT-2

Implementation

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

    1. Date, nature, and purpose of each disclosure; and

    2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

PM-22 Personally Identifiable Information Quality Management

Description

Personally identifiable information quality management includes steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information. Organizational policies and procedures for personally identifiable information quality management are important because inaccurate or outdated personally identifiable information maintained by organizations may cause problems for individuals. Organizations consider the quality of personally identifiable information involved in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or the disclosure of the information may cause stigmatization. Correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of organizations maintaining the information. Organizations consider creating policies and procedures for the removal of such information. The senior agency official for privacy ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information. Processes for correcting or deleting data are clearly defined and publicly available. Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations. Organizations notify individuals or their designated representatives when their personally identifiable information is corrected or deleted to provide transparency and confirm the completed action. Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.

Related Controls

PM-23, SI-18

References

OMB A-130, OMB M-19-15, SP 800-188

Implementation

Develop and document organization-wide policies and procedures for: a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b. Correcting or deleting inaccurate or outdated personally identifiable information; c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d. Appeals of adverse decisions on correction or deletion requests.

PM-23 Data Governance Body

Description

A Data Governance Body can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The Data Governance Body establishes policies, procedures, and standards that facilitate data governance so that data, including personally identifiable information, is effectively managed and maintained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidance. Responsibilities can include developing and implementing guidelines that support data modeling, quality, integrity, and the de-identification needs of personally identifiable information across the information life cycle as well as reviewing and approving applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid.

Members include the chief information officer, senior agency information security officer, and senior agency official for privacy. Federal agencies are required to establish a Data Governance Body with specific roles and responsibilities in accordance with the {#511da9ca-604d-43f7-be41b862085420a9} and policies set forth under

Related Controls

AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19

Implementation

Establish a Data Governance Body consisting of *[Assignment: roles]* with *[Assignment: responsibilities]*.

PM-24 Data Integrity Board

Description

A Data Integrity Board is the board of senior officials designated by the head of a federal agency and is responsible for, among other things, reviewing the agency's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. As a general matter, a matching program is a computerized comparison of records from two or more automated {#18e71fec-c6fd-475a-925a-5d8495cf8455} systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. At a minimum, the Data Integrity Board includes the Inspector General of the agency, if any, and the senior agency official for privacy.

Related Controls

AC-4, PM-19, PM-23, PT-2, PT-8

Implementation

Establish a Data Integrity Board to: a. Review proposals to conduct or participate in a matching program; and b. Conduct an annual review of all matching programs in which the agency has participated.

PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research

Description

The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Organizations consult with the senior agency official for privacy and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder data to avoid exposure of personally identifiable information when conducting testing, training, and research.

Related Controls

PM-23, PT-3, SA-3, SA-8, SI-12

Implementation

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and

d. Review and update policies and procedures *[Assignment: organization-defined frequency]*.

PM-26 Complaint Management

Description

Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the senior agency official for privacy or other official designated to receive complaints. Privacy complaints may also include personally identifiable information which is handled in accordance with relevant policies and processes.

Related Controls

IR-7, IR-9, PM-22, SI-18

Implementation

Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: a. Mechanisms that are easy to use and readily accessible by the public; b. All information necessary for successfully filing complaints; c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within *[Assignment: organization-defined time period]*; d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within *[Assignment: time period]* ; and e. Response to complaints, concerns, or questions from individuals within *[Assignment: time period]*.

PM-27 Privacy Reporting

Description

Through internal and external reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. For federal agencies, privacy reports include annual senior agency official for privacy reports to OMB, reports to Congress required by Implementing Regulations of the 9/11 Commission Act, and other public reports required by law, regulation, or policy, including internal policies of organizations. The senior agency official for privacy consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

Related Controls

IR-9, PM-19

Implementation

a. Develop *[Assignment: privacy reports]* and disseminate to:

   1. *[Assignment: oversight bodies]* to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and

   2. *[Assignment: officials]* and other personnel with responsibility for monitoring privacy program compliance; and

b. Review and update privacy reports *[Assignment: frequency]*.

PM-28 Risk Framing

Description

Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, senior agency information security officer, senior agency official for privacy, and senior accountable official for risk management.

Related Controls

CA-7, PM-9, RA-3, RA-7

Implementation

a. Identify and document:

1. Assumptions affecting risk assessments, risk responses, and risk monitoring;
2. Constraints affecting risk assessments, risk responses, and risk monitoring;
3. Priorities and trade-offs considered by the organization for managing risk; and
4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to *[Assignment: personnel]* ; and

c. Review and update risk framing considerations *[Assignment: frequency]*.

PM-29 Risk Management Program Leadership Roles

Description

The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

Related Controls

PM-2, PM-19

Implementation

a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

PM-30 Supply Chain Risk Management Strategy

Description

An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities. Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization’s overarching risk management

strategy and can guide and inform supply chain policies and system-level supply chain risk management plans. In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-2) is implemented at the system level.

Related Controls

CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11

Implementation

a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implement the supply chain risk management strategy consistently across the organization; and

c. Review and update the supply chain risk management strategy on *[Assignment: frequency]* or as required, to address organizational changes.

PM-30(1) Suppliers of Critical or Mission-essential Items

Description

The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the mission/business success of organizations. The assessment of suppliers is conducted using supplier reviews (see SR-6) and supply chain risk assessment processes (see RA-3(1)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related Controls

RA-3, SR-6

Implementation

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

PM-31 Continuous Monitoring Strategy

Description

Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms

Implementation

Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: *[Assignment: metrics]*; b. Establishing *[Assignment: frequency]* for monitoring and *[Assignment: frequency]* for assessment of control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to *[Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]*.

Related Controls

AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10,

PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4

PM-32 Purposing

Description

Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

Related Controls

CA-7, PL-2, RA-3, RA-9

Implementation

Analyze *[Assignment: systems or system components]* supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Personnel Security – 9 controls

PS-3(1) Classified Information

Description

Classified information is the most sensitive information that the Federal Government processes, stores, or transmits. It is imperative that individuals have the requisite security clearances and system access authorizations prior to gaining access to such information. Access authorizations are enforced by system access controls (see AC-3) and flow controls (see AC-4).

Related Controls

AC-3, AC-4

Implementation

Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

PS-3(2) Formal Indoctrination

Description

Types of classified information that require formal indoctrination include Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartmented Information (SCI).

Related Controls

AC-3, AC-4

Implementation

Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

PS-3(3) Information Requiring Special Protective Measures

Description

Organizational information that requires special protection includes controlled unclassified information. Personnel security criteria include position sensitivity background screening requirements.

Implementation

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

1) Have valid access authorizations that are demonstrated by assigned official government duties; and
2) Satisfy *additional personnel screening criteria*.

PS-3(4) Citizenship Requirements

Description

None.

Implementation

Verify that individuals accessing a system processing, storing, or transmitting *[Assignment: information types]* meet *[Assignment: citizenship requirements]*.

PS-4(1) Post-employment Requirements

Description

Organizations consult with the Office of the General Counsel regarding matters of postemployment requirements on terminated individuals.

Implementation

TAMU-CC shall:

1) Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and
2) Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.

PS-4(2) Automated Actions

Description

In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, electronic mail, text message, or websites. Automated mechanisms can also be employed to quickly and thoroughly disable access to system resources after an employee is terminated.

Implementation

Use *automated mechanisms* to *notify appropriate personnel of individual termination actions and disable access to system resources*.

PS-6(1) Information Requiring Special Protection

Withdrawn: Incorporated into PS-3

PS-6(2) Classified Information Requiring Special Protection

Description

Classified information that requires special protection includes collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Implementation

Verify that access to classified information requiring special protection is granted only to individuals who:

1) Have a valid access authorization that is demonstrated by assigned official government duties;
2) Satisfy associated personnel security criteria; and
3) Have read, understood, and signed a nondisclosure agreement.

PS-6(3) Post-employment Requirements

Description

Organizations consult with the Office of the General Counsel regarding matters of postemployment requirements on terminated individuals.

Related Controls

PS-4

Implementation

TAMU-CC shall:

1) Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and
2) Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

PS-9 Position Descriptions

Description

Specification of security and privacy roles in individual organizational position descriptions facilitates clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Implementation

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Personally Identifiable Information – 19 controls

Processing and Transparency

PT-2 Authority to Process Personally Identifiable Information

Description

The processing of personally identifiable information is an operation or set of operations that the information system or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use,

processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such authority, particularly if the organization is subject to multiple jurisdictions or sources of authority. For organizations whose processing is not determined according to legal authorities, the organization's policies and determinations govern how they process personally identifiable information. While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks. Organizations consider applicable requirements and organizational policies to determine how to document this authority. For federal agencies, the authority to process personally identifiable information is documented in privacy policies and notices, system of records notices, privacy impact assessments, {#18e71fec-c6fd-475a-925a5d8495cf8455} statements, computer matching agreements and notices, contracts, information sharing agreements, memoranda of understanding, and other documentation. Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes, including training organizational personnel on the authorized processing of personally identifiable information and monitoring and auditing organizational use of personally identifiable information.

Related Controls

AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18

References

PRIVACT, OMB A-130, IR 8112

Implementation

TAMU-CC shall:

1) Determine and document the *authority* that permits the *processing* of personally identifiable information; and

2) Restrict the *processing* of personally identifiable information to only that which is authorized.

PT-2(1) Data Tagging

Description

Data tags support the tracking and enforcement of authorized processing by conveying the types of processing that are authorized along with the relevant elements of personally identifiable information throughout the system. Data tags may also support the use of automated tools.

Related Controls

AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19

Implementation

Attach data tags containing *authorized processing* to *elements of personally identifiable information*.

PT-2(2) Automation

Description

Automated mechanisms augment verification that only authorized processing is occurring.

Related Controls

CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19

Implementation

Manage enforcement of the authorized processing of personally identifiable information using *automated mechanisms*.

PT-3(1) Data Tagging

Description

Data tags support the tracking of processing purposes by conveying the purposes along with the relevant elements of personally identifiable information throughout the system. By conveying the processing purposes in a data tag along with the personally identifiable information as the information transits a system, a system owner or operator can identify whether a change in processing would be compatible with the identified and documented purposes. Data tags may also support the use of automated tools.

Related Controls

CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19

Implementation

Attach data tags containing the following purposes to *elements of personally identifiable information*: *[Assignment: processing purposes]*.

PT-3(2) Automation

Description

Automated mechanisms augment tracking of the processing purposes.

Related Controls

CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19

Implementation

Track processing purposes of personally identifiable information using *automated mechanisms*.

PT-4 Consent

Description

Consent allows individuals to participate in making decisions about the processing of their information and transfers some of the risk that arises from the processing of personally identifiable information from the organization to an individual. Consent may be required by applicable laws, executive orders, directives, regulations, policies, standards, or guidelines.

Otherwise, when selecting consent as a control, organizations consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. Organizations consider whether other controls may more effectively mitigate privacy risk either alone or in conjunction with consent. Organizations also consider any demographic or contextual factors that may influence the understanding or behavior of individuals with respect to the processing carried out by the system or organization. When soliciting consent from individuals, organizations consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, organizations consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. Finally, organizations consider usability factors to help individuals understand the risks being accepted when providing consent, including the use of plain language and avoiding technical jargon.

Related Controls

AC-16, PT-2, PT-5

References

PRIVACT, OMB A-130, SP 800-63-3

Implementation

Implement *tools or mechanisms* for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.

PT-4(1) Tailored Consent

Description

While some processing may be necessary for the basic functionality of the product or service, other processing may not. In these circumstances, organizations allow individuals to select how specific personally identifiable information elements may be processed. More tailored consent may help reduce privacy risk, increase individual satisfaction, and avoid adverse behaviors, such as abandonment of the product or service.

Related Controls

PT-2

Implementation

Provide *mechanisms* to allow individuals to tailor processing permissions to selected elements of personally identifiable information.

PT-4(2) Just-in-time Consent

Description

Just-in-time consent enables individuals to participate in how their personally identifiable information is being processed at the time or in conjunction with specific types of data processing when such participation may be most useful to the individual. Individual assumptions about how personally identifiable information is being processed might not be accurate or reliable if time has passed since the individual last gave consent or the type of processing creates significant privacy risk. Organizations use discretion to determine when to use just-in-time consent and may use supporting information on demographics, focus groups, or surveys to learn more about individuals' privacy interests and concerns.

Related Controls

PT-2

Implementation

Present *consent mechanisms* to individuals at *[Assignment: frequency]* and in conjunction with *personally identifiable information processing*.

PT-4(3) Revocation

Description

Revocation of consent enables individuals to exercise control over their initial consent decision when circumstances change. Organizations consider usability factors in enabling easy-to-use revocation capabilities.

Related Controls

PT-2

Implementation

Implement *tools or mechanisms* for individuals to revoke consent to the processing of their personally identifiable information.

PT-5 Privacy Notice

Description

Privacy notices help inform individuals about how their personally identifiable information is being processed by the system or organization. Organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed, as well as other information such as choices individuals might have with respect to that processing and other parties with whom information is shared. Laws, executive orders, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding when and where to provide privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices. Privacy risk assessments identify the privacy risks associated with the processing of personally identifiable information and may help organizations determine appropriate elements to include in a privacy notice to manage such risks. To help individuals understand how their information is being processed, organizations write materials in plain language and avoid technical jargon.

Related Controls

PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18

References

PRIVACT, OMB A-130, OMB A-108

Implementation

Provide notice to individuals about the processing of personally identifiable information that:

1) Is available to individuals upon first interacting with an organization, and subsequently at *[Assignment: frequency]*;
2) Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
3) Identifies the authority that authorizes the processing of personally identifiable information;
4) Identifies the purposes for which personally identifiable information is to be processed; and
5) Includes *[Assignment: information]*.

PT-5(1) Just-in-time Notice

Description

Just-in-time notices inform individuals of how organizations process their personally identifiable information at a time when such notices may be most useful to the individuals. Individual assumptions about how personally identifiable information will be processed might not be accurate or reliable if time has passed since the organization last presented notice or the circumstances under which the individual was last provided notice have changed. A just-in-time notice can explain data actions that organizations have identified as potentially giving rise to greater privacy risk for individuals. Organizations can use a just-in-time notice to update or remind individuals about specific data actions as they occur or highlight specific changes that occurred since last presenting notice. A just-in-time notice can be used in conjunction with just-intime consent to explain what will occur if consent is declined. Organizations use discretion to determine when to use a just-in-time notice and may use supporting information on user demographics, focus groups, or surveys to learn about users' privacy interests and concerns.

Related Controls

PM-21

Implementation

Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or *annually*.

PT-5(2) Privacy Act Statements

Description

If a federal agency asks individuals to supply information that will become part of a system of records, the agency is required to provide a PRIVACT statement on the form used to collect the information or on a separate form that can be retained by the individual. The agency provides a PRIVACT statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond.
PRIVACT statements provide formal notice to individuals of the authority that authorizes the solicitation of the information; whether providing the information is mandatory or voluntary; the principal purpose(s) for which the information is to be used; the published routine uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the information requested; and an appropriate citation and link to the relevant system of records notice. Federal agency personnel consult with the senior agency official for privacy and legal counsel regarding the notice provisions of the {#18e71fec-c6fd-475a925a-5d8495cf8455}.

Related Controls

PT-6

Implementation

Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records or provide Privacy Act statements on separate forms that can be retained by individuals.

PT-6 System of Records Notice

Description

The PRIVACT requires that federal agencies publish a system of records notice in the Federal Register upon the establishment and/or modification of a PRIVACT system of records. As a general matter, a system of records notice is required when an agency maintains a group of any records under the control of the agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier. The notice describes the existence and character of the system and identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system as described in [OMB A-108].

Related Controls

AC-3, PM-20, PT-2, PT-3, PT-5

Implementation

For systems that process information that will be maintained in a Privacy Act system of records:

1) Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;
2) Publish system of records notices in the Federal Register; and
3) Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.

PT-6(1) Routine Uses

Description

A PRIVACT routine use is a particular kind of disclosure of a record outside of the federal agency maintaining the system of records. A routine use is an exception to the PRIVACT prohibition on the disclosure of a record in a system of records without the prior written consent of the individual to whom the record pertains. To qualify as a routine use, the disclosure must be for a purpose that is compatible with the purpose for which the information was originally collected. The PRIVACT requires agencies to describe each routine use of the records maintained in the system of records, including the categories of users of the records and the purpose of the use. Agencies may only establish routine uses by explicitly publishing them in the relevant system of records notice.

Implementation

Review all routine uses published in the system of records notice at least *annually* to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

PT-6(2) Exemption Rules

Description

The PRIVACT includes two sets of provisions that allow federal agencies to claim exemptions from certain requirements in the statute. In certain circumstances, these provisions allow agencies to promulgate regulations to exempt a system of records from select provisions of the PRIVACT. At a minimum, organizations' PRIVACT exemption regulations include the specific name(s) of any system(s) of records that will be exempt, the specific provisions of the PRIVACT from which the system(s) of records is to be exempted, the reasons for the exemption, and an explanation for why the exemption is both necessary and appropriate.

Implementation

Review all Privacy Act exemptions claimed for the system of records at *least annually* to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice.

PT-7 Specific Categories of Personally Identifiable Information

Description

Organizations apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises particular privacy risks. Organizations consult with the senior agency official for privacy and legal counsel regarding any protections that may be necessary.

Related Controls

IR-9, PT-2, PT-3, RA-3

References

PRIVACT, OMB A-130, OMB A-108, NARA CUI

Implementation

Apply *processing conditions* for specific categories of personally identifiable information.

PT-7(1) Social Security Numbers

Description

Federal law and policy establish specific requirements for organizations' processing of Social Security numbers. Organizations take steps to eliminate unnecessary uses of Social Security numbers and other sensitive information and observe any particular requirements that apply.

Related Controls

IA-4

Implementation

When a system processes Social Security numbers:

1) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
2) Do not deny any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his or her Social Security number; and
3) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

PT-7(2) First Amendment Information

Description

The PRIVACT limits agencies' ability to process information that describes how individuals exercise rights guaranteed by the First Amendment. Organizations consult with the senior agency official for privacy and legal counsel regarding these requirements.

Implementation

Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

PT-8 Computer Matching Requirements

Description

The PRIVACT establishes requirements for federal and nonfederal agencies if they engage in a matching program. In general, a matching program is a computerized comparison of records from two or more automated PRIVACT systems of records or an automated system of records and automated records maintained by a non-federal agency (or agent thereof). A matching program either pertains to federal benefit programs or federal personnel or payroll records. A federal benefit match is performed to determine or verify eligibility for payments under federal benefit programs or to recoup payments or delinquent debts under federal benefit programs. A matching program involves not just the matching activity itself but also the investigative follow-up and ultimate action, if any.

Related Controls

PM-24

Implementation

When a system or organization processes information for the purpose of conducting a matching program:

1) Obtain approval from the Data Integrity Board to conduct the matching program;
2) Develop and enter into a computer matching agreement;
3) Publish a matching notice in the Federal Register;

4) Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and
5) Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

Risk Assessment – 16 controls

RA-2(1) Impact-level Prioritization

Description

Organizations apply the

Implementation

Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

RA-3(2) Use of All-source Intelligence

Description

Organizations employ all-source intelligence to inform engineering, acquisition, and risk management decisions. All-source intelligence consists of information derived from all available sources, including publicly available or open-source information, measurement and signature intelligence, human intelligence, signals intelligence, and imagery intelligence. All-source intelligence is used to analyze the risk of vulnerabilities (both intentional and unintentional) from development, manufacturing, and delivery processes, people, and the environment. The risk analysis may be performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Organizations may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.

Implementation

Use all-source intelligence to assist in the analysis of risk.

RA-3(3) Dynamic Threat Awareness

Description

The threat awareness information that is gathered feeds into the organization's information security operations to ensure that procedures are updated in response to the changing threat environment. For example, at higher threat levels, organizations may change the privilege or authentication thresholds required to perform certain operations.

Related Controls

AT-2

Implementation

Determine the current cyber threat environment on an ongoing basis using information sharing & analysis center (ISAC) feeds.

RA-3(4) Predictive Cyber Analytics

Description

A properly resourced Security Operations Center (SOC) or Computer Incident Response Team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and analytics capabilities are typically supported by artificial intelligence concepts, including machine learning. Examples include Automated Threat Discovery and Response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), automated workflow operations, and machine assisted decision tools. Note, however,

that sophisticated adversaries may be able to extract information related to analytic parameters and retrain the machine learning to classify malicious activity as benign. Accordingly, machine learning is augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities.

Implementation

Employ the following advanced automation and analytics capabilities to predict and identify risks to *[Assignment: systems or system components]*: *[Assignment: organization-defined advanced automation and analytics capabilities]*.

RA-4 Risk Assessment Update

Withdrawn: Incorporated into RA-3

RA-5(1) Update Tool Capability

Withdrawn: Incorporated into RA-5

RA-5(2) Update Vulnerabilities to Be Scanned

Description

Due to the complexity of modern software, systems, and other factors, new vulnerabilities are discovered on a regular basis. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related Controls

SI-5

Implementation

Update the system vulnerabilities to be scanned *monthly or prior to a new scan when new vulnerabilities are identified and reported*.

RA-5(3) Breadth and Depth of Coverage

Description

The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element). Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage.

Implementation

Define the breadth and depth of vulnerability scanning coverage.

RA-5(4) Discoverable Information

Description

Discoverable information includes information that adversaries could obtain without compromising or breaching the system, such as by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

Related Controls

AU-13, SC-26

Implementation

Determine information about the system that is discoverable and take *[Assignment: corrective actions]*.

RA-5(5) Privileged Access

Description

In certain situations, the nature of the vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or controlled unclassified information, such as personally identifiable information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Implementation

Implement privileged access authorization to *system components* for *vulnerability scanning activities*.

RA-5(6) Automated Trend Analyses

Description

Using automated mechanisms to analyze multiple vulnerability scans over time can help determine trends in system vulnerabilities and identify patterns of attack.

Implementation

Compare the results of multiple vulnerability scans using *automated mechanisms*.

RA-5(7) Automated Detection and Notification of Unauthorized Components

Withdrawn: Incorporated into CM-8

RA-5(8) Review Historic Audit Logs

Description

Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been previously exploited by an adversary can provide important information for forensic analyses. Such analyses can help identify, for example, the extent of a previous intrusion, the trade craft employed during the attack, organizational information exfiltrated or modified, mission or business capabilities affected, and the duration of the attack.

Related Controls

AU-6, AU-11

Implementation

Review historic audit logs to determine if a vulnerability identified in a *system* has been previously exploited within *seven days*.

RA-5(9) Penetration Testing and Analyses

Withdrawn: Incorporated into CA-8

RA-5(10) Correlate Scanning Information

Description

An attack vector is a path or means by which an adversary can gain access to a system in order to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors. The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and create opportunities for adversary exploitation.

Implementation

Correlate the output from vulnerability scanning tools to determine the presence of multivulnerability and multi-hop attack vectors.

RA-5(11) Public Disclosure Program

Description

The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization does not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific time period to properly remediate the vulnerability.

Implementation

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-6 Technical Surveillance Countermeasures Survey

Description

A technical surveillance countermeasures survey is a service provided by qualified personnel to detect the presence of technical surveillance devices and hazards and to identify technical security weaknesses that could be used in the conduct of a technical penetration of the surveyed facility. Technical surveillance countermeasures surveys also provide evaluations of the technical security posture of organizations and facilities and include visual, electronic, and physical examinations of surveyed facilities, internally and externally. The surveys also provide useful input for risk assessments and information regarding organizational exposure to potential adversaries.

Implementation

Employ a technical surveillance countermeasures survey at *locations when events or indicators warrent*.

RA-8 Privacy Impact Assessments

Description

A privacy impact assessment is an analysis of how personally identifiable information is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A privacy impact assessment is both an analysis and a formal document that details the process and the outcome of the analysis. Organizations conduct and develop a privacy impact assessment with sufficient clarity and specificity to demonstrate that the organization fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the organization’s activity and throughout the information life cycle. In order to conduct a meaningful privacy impact assessment, the organization’s senior agency official for privacy works closely with program managers, system owners, information technology experts, security officials, counsel, and other

relevant organization personnel. Moreover, a privacy impact assessment is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personally identifiable information life cycles. Rather, the privacy analysis continues throughout the system and personally identifiable information life cycles. Accordingly, a privacy impact assessment is a living document that organizations update whenever changes to the information technology, changes to the organization’s practices, or other factors alter the privacy risks associated with the use of such information technology. To conduct the privacy impact assessment, organizations can use security and privacy risk assessments. Organizations may also use other related processes that may have different names, including privacy threshold analyses. A privacy impact assessment can also serve as notice to the public regarding the organization’s practices with respect to privacy. Although conducting and publishing privacy impact assessments may be required by law, organizations may develop such policies in the absence of applicable laws. For federal agencies, privacy impact assessments may be required by {#7b0b9634-741a-4335-b6fa-161228c3a76e} ; agencies should consult with their senior agency official for privacy and legal counsel on this requirement and be aware of the statutory exceptions and OMB guidance relating to the provision.

Related Controls

CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7

References

EGOV, OMB A-130, OMB M-03-22

Implementation

Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes personally identifiable information; and b. Initiating a new collection of personally identifiable information that:

1) Will be processed using information technology; and
2) Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

RA-9 Criticality Analysis

Description

Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system. The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber-physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions. Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality

analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.

Related Controls

CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5

References

IR 8179

Implementation

Identify critical system components and functions by performing a criticality analysis for *systems, system components, or system services* at *decision points in the system development life cycle*.

RA-10 Threat Hunting

Description

Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and

Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

Related Controls

CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4

Implementation

TAMU-CC shall:

1) Establish and maintain a cyber threat hunting capability to:

    a) Search for indicators of compromise in organizational systems; and

    b) Detect, track, and disrupt threats that evade existing controls; and

2) Employ the threat hunting capability upon detection.

System and Services Acquisition – 96 controls

SA-3(1) Manage Preproduction Environment

Description

The preproduction environment includes development, test, and integration environments. The program protection planning processes established by the Department of Defense are examples of managing the preproduction environment for defense contractors. Criticality analysis and the application of controls on developers also contribute to a more secure system development environment.

Related Controls

CM-2, CM-4, RA-3, RA-9, SA-4

Implementation

Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.

SA-3(2) Use of Live or Operational Data

Description

Live data is also referred to as operational data. The use of live or operational data in preproduction (i.e., development, test, and integration) environments can result in significant risks to organizations. In addition, the use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information.
Therefore, it is important for the organization to manage any additional risks that may result from the use of live or operational data. Organizations can minimize such risks by using test or dummy data during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable.

Related Controls

PM-25, RA-3

Implementation

TAMU-CC shall:

1) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and

2) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

SA-3(3) Technology Refresh

Description

Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components, counterfeit or repurposed components, components unable to implement security or privacy requirements, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity. Technology refreshes typically occur during the operations and maintenance stage of the system development life cycle.

Related Controls

MA-6

Implementation

Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

SA-4(1) Functional Properties of Controls

Description

Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Implementation

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

SA-4(2) Design and Implementation Information for Controls

Description

Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Implementation

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes:

1) *Security relevant external system interfaces;*
2) *high-level design;*
3) *low-level design;*
4) *source code or hardware schematics*.

SA-4(3) Development Methods, Techniques, and Practices

Description

Following a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Transparency in the methods and techniques that developers select and implement for systems engineering, systems security and privacy engineering, software development, component and system assessments, and quality control processes provides an increased level of assurance in the trustworthiness of the system, system component, or system service being acquired.

Implementation

Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:

1) *systems engineering methods*;
2) *system security engineering methods;*
3) *privacy engineering methods* ;
4) *software development methods;*
5) *testing, evaluation, assessment, verification, and validation methods; and*
6) *quality control processes*.

SA-4(4) Assignment of Components to Systems

Withdrawn: Incorporated into CM-8.9

SA-4(5) System, Component, and Service Configurations

Description

Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

Implementation

Require the developer of the system, system component, or system service to:

1) Deliver the system, component, or service with *security configurations* implemented; and
2) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

SA-4(6) Use of Information Assurance Products

Description

Commercial off-the-shelf IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. See

Related Controls

SC-8, SC-12, SC-13

Implementation

TAMU-CC shall:

1) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved

solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

2) Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.

SA-4(7) Niap-approved Protection Profiles

Description

See [NIAP CCEVS] for additional information on NIAP. See [NIST CMVP] for additional information on FIPS-validated cryptographic modules.

Related Controls:

IA-7, SC-12, SC-13.

Implementation

TAMU-CC shall:

1) Limit the use of commercially provided information assurance and information assurance enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and
2) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.

SA-4(8) Continuous Monitoring Plan for Controls

Description

The objective of continuous monitoring plans is to determine if the planned, required, and deployed controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a

sufficient level of detail such that the information can be incorporated into continuous monitoring programs implemented by organizations. Continuous monitoring plans can include the types of control assessment and monitoring activities planned, frequency of control monitoring, and actions to be taken when controls fail or become ineffective.

Related Controls

CA-7

Implementation

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

SA-4(9) Functions, Ports, Protocols, and Services in Use

Description

The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related Controls

CM-7, SA-9

Implementation

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

SA-4(10) Use of Approved PIV Products

Description

Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations.

Related Controls

IA-2, IA-8, PM-9

Implementation

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

SA-4(11) System of Records

Description

When, by contract, an organization provides for the operation of a system of records to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirements of the [PRIVACT] to be applied to the system of records.

Related Controls

PT-6

Implementation

Include *Privacy Act requirements* in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.

SA-4(12) Data Ownership

Description

Contractors who operate a system that contains data owned by an organization initiating the contract have policies and procedures in place to remove the data from their systems and/or return the data in a time frame defined by the contract.

Implementation

TAMU-CC shall:

1) Include organizational data ownership requirements in the acquisition contract; and
2) Require all data to be removed from the contractor's system and returned to the organization within thirty (30) days.

SA-5(1) Functional Properties of Security Controls

Withdrawn: Incorporated into SA-4.1

SA-5(2) Security-relevant External System Interfaces

Withdrawn: Incorporated into SA-4.2

SA-5(3) High-level Design

Withdrawn: Incorporated into SA-4.2

SA-5(4) Low-level Design

Withdrawn: Incorporated into SA-4.2

SA-5(5) Source Code

Withdrawn: Incorporated into SA-4.2

SA-6 Software Usage Restrictions

Withdrawn: Incorporated into CM-10, SI-7

SA-7 User-installed Software

Withdrawn: Incorporated into CM-11, SI-7

SA-8(1) Clear Abstractions

Description

The principle of clear abstractions states that a system has simple, well-defined interfaces and functions that provide a consistent and intuitive view of the data and how the data is managed. The clarity, simplicity, necessity, and sufficiency of the system interfaces- combined with a precise definition of their functional behavior-promotes ease of analysis, inspection, and testing as well as the correct and secure use of the system. The clarity of an abstraction is subjective. Examples that reflect the application of this principle include avoidance of redundant, unused interfaces; information hiding; and avoidance of semantic overloading of interfaces or their parameters. Information hiding (i.e., representation-independent programming), is a design discipline used to ensure that the internal representation of information in one system component is not visible to

another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.

Implementation

Implement the security design principle of clear abstractions.

SA-8(2) Least Common Mechanism

Description

The principle of least common mechanism states that the amount of mechanism common to more than one user and depended on by all users is minimized {#79453f84-26a4-4995-8257d32d37aefea3} . Mechanism minimization implies that different components of a system refrain from using the same mechanism to access a system resource. Every shared mechanism (especially a mechanism involving shared variables) represents a potential information path between users and is designed with care to ensure that it does not unintentionally compromise security {#c9495d6e-ef64-4090-8509-e58c3b9009ff} . Implementing the principle of least

common mechanism helps to reduce the adverse consequences of sharing the system state among different programs. A single program that corrupts a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels {#d1cdab13-4218-400d-91a9-c3818dfa5ec8}.

Implementation

Implement the security design principle of least common mechanism in *systems or system components*.

SA-8(3) Modularity and Layering

Description

The principles of modularity and layering are fundamental across system engineering disciplines. Modularity and layering derived from functional decomposition are effective in managing system complexity by making it possible to comprehend the structure of the system. Modular decomposition, or refinement in system design, is challenging and resists general statements of principle. Modularity serves to isolate functions and related data structures into well-defined logical units. Layering allows the relationships of these units to be better understood so that dependencies are clear and undesired complexity can be avoided. The security design principle of modularity extends functional modularity to include considerations based on trust, trustworthiness, privilege, and security policy. Security-informed modular decomposition includes the allocation of policies to systems in a network, separation of system applications into processes with distinct address spaces, allocation of system policies to layers, and separation of processes into subjects with distinct privileges based on hardware-supported privilege domains.

Related Controls

SC-2, SC-3

Implementation

Implement the security design principles of modularity and layering in *systems or system components*.

SA-8(4) Partially Ordered Dependencies

Description

The principle of partially ordered dependencies states that the synchronization, calling, and other dependencies in the system are partially ordered. A fundamental concept in system design is layering, whereby the system is organized into well-defined, functionally related modules or

components. The layers are linearly ordered with respect to inter-layer dependencies, such that higher layers are dependent on lower layers. While providing functionality to higher layers, some layers can be self-contained and not dependent on lower layers. While a partial ordering of all functions in a given system may not be possible, if circular dependencies are constrained to occur within layers, the inherent problems of circularity can be more easily managed. Partially ordered dependencies and system layering contribute significantly to the simplicity and coherency of the system design. Partially ordered dependencies also facilitate system testing and analysis.

Implementation

Implement the security design principle of partially ordered dependencies in *systems or system components*.

SA-8(5) Efficiently Mediated Access

Description

The principle of efficiently mediated access states that policy enforcement mechanisms utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints. The mediation of access to system resources (i.e., CPU, memory, devices, communication ports, services, infrastructure, data, and information) is often the predominant security function of secure systems. It also enables the realization of protections for the capability provided to stakeholders by the system. Mediation of resource access can result in performance bottlenecks if the system is not designed correctly. For example, by using hardware mechanisms, efficiently mediated access can be achieved. Once access to a low-level resource such as memory has been obtained, hardware protection mechanisms can ensure that out-of-bounds access does not occur.

Related Controls

AC-25

Implementation

Implement the security design principle of efficiently mediated access in *systems or system components*.

SA-8(6) Minimized Sharing

Description

The principle of minimized sharing states that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify system design and implementation. In order to protect user domain resources from arbitrary active entities, no resource is shared unless that sharing has been explicitly requested and granted. The need for resource sharing can be motivated by the design principle of least common mechanism in the case of internal entities or driven by stakeholder requirements. However, internal sharing is carefully designed to avoid performance and covert storage and timing channel problems. Sharing via common mechanism can increase the susceptibility of data and information to unauthorized access, disclosure, use, or modification and can adversely affect the inherent capability provided by the system. To minimize sharing induced by common mechanisms, such mechanisms can be designed to be reentrant or virtualized to preserve separation. Moreover, the use of global data to share information is carefully scrutinized. The lack of encapsulation may obfuscate relationships among the sharing entities.

Related Controls

SC-31

Implementation

Implement the security design principle of minimized sharing in *systems or system components*.

SA-8(7) Reduced Complexity

Description

The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more analyzable, and less prone to error. The reduced complexity principle applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential. Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain; that is, simpler systems contain fewer vulnerabilities. An benefit of reduced complexity is that it is easier to understand whether the intended security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and the existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex. Transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6) may require implementing the older and newer technologies simultaneously during the transition period. This may result in a temporary increase in system complexity during the transition.

Implementation

Implement the security design principle of reduced complexity in *systems or system components*.

SA-8(8) Secure Evolvability

Description

The principle of secure evolvability states that a system is developed to facilitate the maintenance of its security properties when there are changes to the system's structure, interfaces, interconnections (i.e., system architecture), functionality, or configuration (i.e., security policy enforcement). Changes include a new, enhanced, or upgraded system capability; maintenance and sustainment activities; and reconfiguration. Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic direction, anticipated changes in the threat environment, and anticipated maintenance and sustainment needs. It is unrealistic to expect that complex systems remain secure in contexts not envisioned during development, whether such contexts are related to the operational environment or to usage. A system may be secure in some new contexts, but there is no guarantee that its emergent behavior will always be secure. It is easier to build trustworthiness into a system from the outset, and it follows that the sustainment of system trustworthiness requires planning for change as opposed to adapting in an ad hoc or non-methodical manner. The benefits of this principle include reduced vendor life cycle costs, reduced cost of ownership, improved system security, more effective management of security risk, and less risk uncertainty.

Related Controls

CM-3

Implementation

Implement the security design principle of secure evolvability in *systems or system components*.

SA-8(9) Trusted Components

Description

The principle of trusted components states that a component is trustworthy to at least a level commensurate with the security dependencies it supports (i.e., how much it is trusted to perform its security functions by other components). This principle enables the composition of components such that trustworthiness is not inadvertently diminished and the trust is not consequently misplaced. Ultimately, this principle demands some metric by which the trust in a component and the trustworthiness of a component can be measured on the same abstract scale. The principle of trusted components is particularly relevant when considering systems and components in which there are complex chains of trust dependencies. A trust dependency is also referred to as a trust relationship and there may be chains of trust relationships. The principle of trusted components also applies to a compound component that consists of subcomponents (e.g., a subsystem), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is that of its least trustworthy subcomponent. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than the conservative assumption. However, any such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives as well as relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defense-in-depth layering within the component or a replication of components. Defense-in-depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.

Implementation

Implement the security design principle of trusted components in *systems or system components*.

SA-8(10) Hierarchical Trust

Description

The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for trustworthiness reasoning or an assurance case (assurance argument) when composing a secure system from heterogeneously trustworthy components. To analyze a system composed of heterogeneously trustworthy components for its trustworthiness, it is essential to eliminate circular dependencies with regard to the trustworthiness. If a more trustworthy component located in a lower layer of the system were to depend on a less trustworthy component in a higher layer, this would, in effect, put the components in the same

Implementation

Implement the security design principle of hierarchical trust in *systems or system components*.

SA-8(11) Inverse Modification Threshold

Description

The principle of inverse modification threshold builds on the principle of trusted components and the principle of hierarchical trust and states that the degree of protection provided to a component is commensurate with its trustworthiness. As the trust placed in a component increases, the protection against unauthorized modification of the component also increases to the same degree. Protection from unauthorized modification can come in the form of the component’s own self-protection and innate trustworthiness, or it can come from the protections afforded to the component from other elements or attributes of the security architecture (to include protections in the environment of operation).

Implementation

Implement the security design principle of inverse modification threshold in *systems or system components*.

SA-8(12) Hierarchical Protection

Description

The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted component, it protects itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it protects itself from all untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel. The trustworthiness of users is a consideration for applying the principle of hierarchical protection. A trusted system need not protect itself from an equally trustworthy user, reflecting use of untrusted systems in

Implementation

Implement the security design principle of hierarchical protection in *systems or system components*.

SA-8(13) Minimized Security Elements

Description

The principle of minimized security elements states that the system does not have extraneous trusted components. The principle of minimized security elements has two aspects: the overall cost of security analysis and the complexity of security analysis. Trusted components are generally costlier to construct and implement, owing to the increased rigor of development processes. Trusted components require greater security analysis to qualify their trustworthiness. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trustworthy components as possible. The analysis of the interaction of trusted components with other

components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to ascertain than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.

Implementation

Implement the security design principle of minimized security elements in *systems or system components*.

SA-8(14) Least Privilege

Description

The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has need to view the audit data that has been collected but no need to perform operations on that data. In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated on by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements.

Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality and that the access modes for the elements (e.g., read, write) are minimal.

Related Controls

AC-6, CM-7

Implementation

Implement the security design principle of least privilege in *systems or system components*.

SA-8(15) Predicate Permission

Description

The principle of predicate permission states that system designers consider requiring multiple authorized entities to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is allowed to proceed. {#c9495d6e-ef64-4090-8509e58c3b9009ff} originally named predicate permission the separation of privilege. It is also equivalent to separation of duty. The division of privilege among multiple parties decreases the likelihood of abuse and provides the safeguard that no single accident, deception, or breach of trust is sufficient to enable an unrecoverable action that can lead to significantly damaging effects. The design options for such a mechanism may require simultaneous action (e.g., the firing of a nuclear weapon requires two different authorized individuals to give the correct command within a small time window) or a sequence of operations where each successive action is enabled by some prior action, but no single individual is able to enable more than one action.

Related Controls

AC-5

Implementation

Implement the security design principle of predicate permission in *systems or system components*.

SA-8(16) Self-reliant Trustworthiness

Description

The principle of self-reliant trustworthiness states that systems minimize their reliance on other systems for their own trustworthiness. A system is trustworthy by default, and any connection to an external entity is used to supplement its function. If a system were required to maintain a connection with another external entity in order to maintain its trustworthiness, then that system would be vulnerable to malicious and non-malicious threats that could result in the loss or degradation of that connection. The benefit of the principle of self-reliant trustworthiness is that the isolation of a system will make it less vulnerable to attack. A corollary to this principle relates to the ability of the system (or system component) to operate in isolation and then resynchronize with other components when it is rejoined with them.

Implementation

Implement the security design principle of self-reliant trustworthiness in *systems or system components*.

SA-8(17) Secure Distributed Composition

Description

The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy result in a system that enforces that policy at least as well as the individual components do. Many of the design principles for secure systems deal with how components can or should interact. The need to create or enable a capability from the composition of distributed components can magnify the relevancy of these principles. In particular, the translation of security policy from a stand-alone to a distributed system or a system-

of-systems can have unexpected or emergent results. Communication protocols and distributed data consistency mechanisms help to ensure consistent policy enforcement across a distributed system. To ensure a system-wide level of assurance of correct policy enforcement, the security architecture of a distributed composite system is thoroughly analyzed.

Implementation

Implement the security design principle of secure distributed composition in *systems or system components*.

SA-8(18) Trusted Communications Channels

Description

The principle of trusted communication channels states that when composing a system where there is a potential threat to communications between components (i.e., the interconnections between components), each communication channel is trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions). Trusted communication channels are achieved by a combination of restricting access to the communication channel (to ensure an acceptable match in the trustworthiness of the endpoints involved in the communication) and employing end-to-end protections for the data transmitted over the communication channel (to protect against interception and modification and to further increase the assurance of proper end-to-end communication).

Related Controls

SC-8, SC-12, SC-13

Implementation

Implement the security design principle of trusted communications channels in *systems or system components*.

SA-8(19) Continuous Protection

Description

The principle of continuous protection states that components and data used to enforce the security policy have uninterrupted protection that is consistent with the security policy and the security architecture assumptions. No assurances that the system can provide the confidentiality, integrity, availability, and privacy protections for its design capability can be made if there are gaps in the protection. Any assurances about the ability to secure a delivered capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unprotected while under control of the system (i.e., during the creation, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruption, and shutdown). Continuous protection requires adherence to the precepts of the reference monitor concept (i.e., every request is validated by the reference monitor; the reference monitor is able to protect itself from tampering; and sufficient assurance of the correctness and completeness of the mechanism can be ascertained from analysis and testing) and the principle of secure failure and recovery (i.e., preservation of a secure state during error, fault, failure, and successful attack; preservation of a secure state during recovery to normal, degraded, or alternative operational modes). Continuous protection also applies to systems designed to operate in varying configurations, including those that deliver full operational capability and degraded-mode configurations that deliver partial operational capability. The continuous protection principle requires that changes to the system security policies be traceable to the operational need that drives the configuration and be verifiable (i.e., it is possible to verify that the proposed changes will not put the system into an insecure state). Insufficient traceability and verification may lead to inconsistent states or protection discontinuities due to the complex or undecidable nature of the problem. The use of pre-verified configuration definitions that reflect the new security policy enables analysis to determine that a transition from old to new policies is essentially atomic and that any residual effects from the old policy are guaranteed to not conflict with the new policy. The ability to demonstrate continuous protection is rooted in the clear articulation of life cycle protection needs as stakeholder security requirements.

Related Controls

AC-25

Implementation

Implement the security design principle of continuous protection in *systems or system components*.

SA-8(20) Secure Metadata Management

Description

The principle of secure metadata management states that metadata are The apparent secondary nature of metadata can lead to neglect of its legitimate need for protection, resulting in a violation of the security policy that includes the exfiltration of information. A particular concern associated with insufficient protections for metadata is associated with multilevel secure (MLS) systems. MLS systems mediate access by a subject to an object based on relative sensitivity levels. It follows that all subjects and objects in the scope of control of the MLS system are either directly labeled or indirectly attributed with sensitivity levels. The corollary of labeled metadata for MLS systems states that objects containing metadata are labeled. As with protection needs assessments for data, attention is given to ensure that the confidentiality and integrity protections are individually assessed, specified, and allocated to metadata, as would be done for mission, business, and system data.

Implementation

Implement the security design principle of secure metadata management in *systems or system components*.

SA-8(21) Self-analysis

Description

The principle of self-analysis states that a system component is able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability is commensurate with the level of trustworthiness invested in the system. At the system level, self-analysis can be achieved through hierarchical assessments of trustworthiness established in a bottom-up fashion. In this approach, the lower-level components check for data integrity and correct functionality (to a limited extent) of higher-level components. For example, trusted boot sequences involve a trusted lower-level component that attests to the trustworthiness of the next higher-level components so that a transitive chain of trust can be established. At the root, a component attests to itself, which usually involves an axiomatic or environmentally enforced assumption about its integrity. Results of the self-analyses can be used to guard against externally induced errors, internal malfunction, or transient errors. By following this principle, some simple malfunctions or errors can be detected without allowing the effects of the error or malfunction to propagate outside of the component. Further, the self-test can be used to attest to the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.

Related Controls

CA-7

Implementation

Implement the security design principle of self-analysis in *systems or system components*.

SA-8(22) Accountability and Traceability

Description

The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-object interactions) to the entity on whose behalf the action is being taken. The

principle of accountability and traceability requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., an audit subsystem). To record the details about actions, the system is able to uniquely identify the entity on whose behalf the action is being carried out and also record the relevant sequence of actions that are carried out. The accountability policy also requires that audit trail itself be protected from unauthorized access and modification. The principle of least privilege assists in tracing the actions to particular entities, as it increases the granularity of accountability. Associating specific actions with system entities, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provide non-repudiation because once an action is recorded, it is not possible to change the audit trail. Another important function that accountability and traceability serves is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or component that allowed the violation of the security policy and the actions of individuals associated with the violation of the security policy.

Related Controls

AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4

Implementation

Implement the security design principle of accountability and traceability in *systems or system components*.

SA-8(23) Secure Defaults

Description

The principle of secure defaults states that the default configuration of a system (including its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults applies to the initial (i.e., default) configuration of a system as well as to the security engineering and design of access control and other security functions that follow a Restrictive defaults mean that the system will operate The security engineering approach to this principle states that security mechanisms deny requests

unless the request is found to be well-formed and consistent with the security policy. The insecure alternative is to allow a request unless it is shown to be inconsistent with the policy. In a large system, the conditions that are satisfied to grant a request that is denied by default are often far more compact and complete than those that would need to be checked in order to deny a request that is granted by default.

Related Controls

CM-2, CM-6, SA-4

Implementation

Implement the security design principle of secure defaults in *systems or system components*.

SA-8(24) Secure Failure and Recovery

Description

The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The principle of secure failure and recovery parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated. In addition, when specified, the system is capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operations while ensuring that a secure state is maintained such that security policies are not violated. Failure is a condition in which the behavior of a component deviates from its specified or expected behavior for an explicitly documented input. Once a failed security function is detected, the system may reconfigure itself to circumvent the failed component while maintaining security and provide all or part of the functionality of the original system, or it may completely shut itself down to prevent any further violation of security policies. For this to occur, the reconfiguration functions of the system are designed to ensure continuous enforcement of security policy during the various phases of reconfiguration. Another technique that can be used to recover from failures is to perform

a rollback to a secure state (which may be the initial state) and then either shutdown or replace the service or component that failed such that secure operations may resume. Failure of a component may or may not be detectable to the components using it. The principle of secure failure indicates that components fail in a state that denies rather than grants access. For example, a nominally Failure protection strategies that employ replication of policy enforcement mechanisms, sometimes called defense in depth, can allow the system to continue in a secure state even when one mechanism has failed to protect the system. If the mechanisms are similar, however, the additional protection may be illusory, as the adversary can simply attack in series. Similarly, in a networked system, breaking the security on one system or service may enable an attacker to do the same on other similar replicated systems and services. By employing multiple protection mechanisms whose features are significantly different, the possibility of attack replication or repetition can be reduced. Analyses are conducted to weigh the costs and benefits of such redundancy techniques against increased resource usage and adverse effects on the overall system performance. Additional analyses are conducted as the complexity of these mechanisms increases, as could be the case for dynamic behaviors. Increased complexity generally reduces trustworthiness. When a resource cannot be continuously protected, it is critical to detect and repair any security breaches before the resource is once again used in a secure context.

Related Controls

CP-10, CP-12, SC-7, SC-8, SC-24, SI-13

Implementation

Implement the security design principle of secure failure and recovery in *systems or system components*.

SA-8(25) Economic Security

Description

The principle of economic security states that security mechanisms are not costlier than the potential damage that could occur from a security breach. This is the security-relevant form of the cost-benefit analyses used in risk management. The cost assumptions of cost-benefit analysis

prevent the system designer from incorporating security mechanisms of greater strength than necessary, where strength of mechanism is proportional to cost. The principle of economic security also requires analysis of the benefits of assurance relative to the cost of that assurance in terms of the effort expended to obtain relevant and credible evidence as well as the necessary analyses to assess and draw trustworthiness and risk conclusions from the evidence.

Related Controls

RA-3

Implementation

Implement the security design principle of economic security in *systems or system components*.

SA-8(26) Performance Security

Description

The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized. For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers adhere to the specified constraints that capability performance needs place on protection needs. The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection. The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat. The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware

mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory is granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode. Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.

Related Controls

SC-12, SC-13, SI-2, SI-7

Implementation

Implement the security design principle of performance security in *systems or system components*.

SA-8(27) Human Factored Security

Description

The principle of human factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions that affect such policy and its enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency. Security policy enforcement mechanisms also provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made. Particular attention is given to interfaces through which personnel responsible for system administration and operation configure and set up the security policies. Ideally, these personnel are able to understand the impact of their choices. Personnel with system administrative and operational responsibilities are able to configure systems before start-up and administer them during runtime with confidence that their intent is correctly mapped to the system’s mechanisms. Security services, functions, and mechanisms do not impede or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the strictness necessary for security policy enforcement. If security mechanisms are frustrating or difficult to use,

then users may disable them, avoid them, or use them in ways inconsistent with the security requirements and protection needs that the mechanisms were designed to satisfy.

Implementation

Implement the security design principle of human factored security in *systems or system components*.

SA-8(28) Acceptable Security

Description

The principle of acceptable security requires that the level of privacy and performance that the system provides is consistent with the users' expectations. The perception of personal privacy may affect user behavior, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces or meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.

Implementation

Implement the security design principle of acceptable security in *systems or system components*.

SA-8(29) Repeatable and Documented Procedures

Description

The principle of repeatable and documented procedures states that the techniques and methods employed to construct a system component permit the same component to be completely and correctly reconstructed at a later time. Repeatable and documented procedures support the development of a component that is identical to the component created earlier, which may be in widespread use. In the case of other system artifacts (e.g., documentation and testing results), repeatability supports consistency and the ability to inspect the artifacts. Repeatable and

documented procedures can be introduced at various stages within the system development life cycle and contribute to the ability to evaluate assurance claims for the system. Examples include systematic procedures for code development and review, procedures for the configuration management of development tools and system artifacts, and procedures for system delivery.

Related Controls

CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1

Implementation

Implement the security design principle of repeatable and documented procedures in *systems or system components*.

SA-8(30) Procedural Rigor

Description

The principle of procedural rigor states that the rigor of a system life cycle process is commensurate with its intended trustworthiness. Procedural rigor defines the scope, depth, and detail of the system life cycle procedures. Rigorous system life cycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the life cycle process such that the introduction of unspecified functionality is prevented. Second, rigorous procedures applied to systems security engineering activities that produce specifications and other system design documents contribute to the ability to understand the system as it has been built rather than trusting that the component, as implemented, is the authoritative (and potentially misleading) specification. Finally, modifications to an existing system component are easier when there are detailed specifications that describe its current design instead of studying source code or schematics to try to understand how it works. Procedural rigor helps ensure that security functional and assurance requirements have been satisfied, and it contributes to a better-informed basis for the determination of trustworthiness and risk posture. Procedural rigor is commensurate with the degree of assurance desired for the system. If the required trustworthiness of the system is low, a high level of

procedural rigor may add unnecessary cost, whereas when high trustworthiness is critical, the cost of high procedural rigor is merited.

Implementation

Implement the security design principle of procedural rigor in *systems or system components*.

SA-8(31) Secure System Modification

Description

The principle of secure system modification states that system modification maintains system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform secure systems into systems that are not secure. The procedures for system modification ensure that if the system is to maintain its trustworthiness, the same rigor that was applied to its initial development is applied to any system changes. Because modifications can affect the ability of the system to maintain its secure state, a careful security analysis of the modification is needed prior to its implementation and deployment. This principle parallels the principle of secure evolvability.

Related Controls

CM-3, CM-4

Implementation

Implement the security design principle of secure system modification in *systems or system components*.

SA-8(32) Sufficient Documentation

Description

The principle of sufficient documentation states that organizational personnel with responsibilities to interact with the system are provided with adequate documentation and other information such that the personnel contribute to rather than detract from system security. Despite attempts to comply with principles such as human factored security and acceptable security, systems are inherently complex, and the design intent for the use of security mechanisms and the ramifications of the misuse or misconfiguration of security mechanisms are not always intuitively obvious. Uninformed and insufficiently trained users can introduce vulnerabilities due to errors of omission and commission. The availability of documentation and training can help to ensure a knowledgeable cadre of personnel, all of whom have a critical role in the achievement of principles such as continuous protection. Documentation is written clearly and supported by training that provides security awareness and understanding of security-relevant responsibilities.

Related Controls

AT-2, AT-3, SA-5

Implementation

Implement the security design principle of sufficient documentation in s*ystems or system components*.

SA-8(33) Minimization

Description

The principle of minimization states that organizations should only process personally identifiable information that is directly relevant and necessary to accomplish an authorized purpose and should only maintain personally identifiable information for as long as is necessary to accomplish the

purpose. Organizations have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

Related Controls

PE-8, PM-25, SC-42, SI-12

Implementation

Implement the privacy principle of minimization using *security and privacy processes*.

SA-9(1) Risk Assessments and Organizational Approvals

Description

Information security services include the operation of security devices, such as firewalls or key management services as well as incident monitoring, analysis, and response. Risks assessed can include system, mission or business, security, privacy, or supply chain risks.

Related Controls

CA-6, RA-3, RA-8

Implementation

TAMU-CC shall:

1) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and
2) Verify that the acquisition or outsourcing of dedicated information security services is approved by the Office of Information Security.

SA-9(2) Identification of Functions, Ports, Protocols, and Services

Description

Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related Controls

CM-6, CM-7

Implementation

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: *[Assignment: external system services]*.

SA-9(3) Establish and Maintain Trust Relationship with Providers

Description

Trust relationships between organizations and external service providers reflect the degree of confidence that the risk from using external services is at an acceptable level. Trust relationships can help organizations gain increased levels of confidence that service providers are providing adequate protection for the services rendered and can also be useful when conducting incident response or when planning for upgrades or obsolescence. Trust relationships can be complicated due to the potentially large number of entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control that organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or

individual privacy and the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements.

Related Controls

SR-2

Implementation

Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions:

1) *security and privacy requirements, properties, factors; or*
2) *conditions defining acceptable trust relationships*.

SA-9(4) Consistent Interests of Consumers and Providers

Description

As organizations increasingly use external service providers, it is possible that the interests of the service providers may diverge from organizational interests. In such situations, simply having the required technical, management, or operational controls in place may not be sufficient if the providers that implement and manage those controls are not operating in a manner consistent with the interests of the consuming organizations. Actions that organizations take to address such concerns include requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, such as providers with which organizations have had successful trust relationships; and conducting routine, periodic, unscheduled visits to service provider facilities.

Implementation

Take the following actions to verify that the interests of *external service providers* are consistent with and reflect organizational interests: *[Assignment: actions]*.

SA-9(5) Processing, Storage, and Service Location

Description

The location of information processing, information and data storage, or system services can have a direct impact on the ability of organizations to successfully execute their mission and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use for the selection of processing, storage, or service locations may be different from the criteria that organizations use. For example, organizations may desire that data or information storage locations be restricted to certain locations to help facilitate incident response activities in case of information security incidents or breaches. Incident response activities, including forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws, policies, or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

Related Controls

SA-5, SR-4

Implementation

Restrict the location of *information processing, information or data, system services* to a designated data center based on *data categorization requirements.*

SA-9(6) Organization-controlled Cryptographic Keys

Description

Maintaining exclusive control of cryptographic keys in an external system prevents decryption of organizational data by external system staff. Organizational control of cryptographic keys can be implemented by encrypting and decrypting data inside the organization as data is sent to and received from the external system or by employing a component that permits encryption and

decryption functions to be local to the external system but allows exclusive organizational access to the encryption keys.

Related Controls

SC-12, SC-13, SI-4

Implementation

Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

SA-9(7) Organization-controlled Integrity Checking

Description

Storage of organizational information in an external system could limit visibility into the security status of its data. The ability of the organization to verify and validate the integrity of its stored data without transferring it out of the external system provides such visibility.

Related Controls

SI-7

Implementation

Provide the capability to check the integrity of information while it resides in the external system.

SA-9(8) Processing and Storage Location - U.S. Jurisdiction

Description

The geographic location of information processing and data storage can have a direct impact on the ability of organizations to successfully execute their mission and business functions. A compromise

or breach of high impact information and systems can have severe or catastrophic adverse impacts on organizational assets and operations, individuals, other organizations, and the Nation. Restricting the processing and storage of high-impact information to facilities within the legal jurisdictional boundary of the United States provides greater control over such processing and storage.

Related Controls

SA-5, SR-4

Implementation

Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

SA-10(1) Software and Firmware Integrity Verification

Description

Software and firmware integrity verification allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. The integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

Related Controls

SI-7, SR-11

Implementation

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

SA-10(2) Alternative Configuration Management Processes

Description

Alternate configuration management processes may be required when organizations use commercial off-the-shelf information technology products. Alternate configuration management processes include organizational personnel who review and approve proposed changes to systems, system components, and system services and conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services.

Implementation

Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

SA-10(3) Hardware Integrity Verification

Description

Hardware integrity verification allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations may verify the integrity of hardware components with hard-to-copy labels, verifiable serial numbers provided by developers, and by requiring the use of anti-tamper technologies. Delivered hardware components also include hardware and firmware updates to such components.

Related Controls

SI-7

Implementation

Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

SA-10(4) Trusted Generation

Description

The trusted generation of descriptions, source code, and object code addresses authorized changes to hardware, software, and firmware components between versions during development. The focus is on the efficacy of the configuration management process by the developer to ensure that newly generated versions of security-relevant hardware descriptions, source code, and object code continue to enforce the security policy for the system, system component, or system service. In contrast, SA-10(1) and SA-10(3) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, or mechanisms provided by developers.

Implementation

Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.

SA-10(5) Mapping Integrity for Version Control

Description

Mapping integrity for version control addresses changes to hardware, software, and firmware components during both initial development and system development life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs, hardware drawings, source code) and the equivalent data in master

copies in operational environments is essential to ensuring the availability of organizational systems that support critical mission and business functions.

Implementation

Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security relevant hardware, software, and firmware and the on-site master copy of the data for the current version.

SA-10(6) Trusted Distribution

Description

The trusted distribution of security-relevant hardware, software, and firmware updates help to ensure that the updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.

Implementation

Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

SA-10(7) Security and Privacy Representatives

Description

Information security and privacy representatives can include system security officers, senior agency information security officers, senior agency officials for privacy, and system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of

systems. The configuration change management and control process in this control enhancement refers to the change management and control process defined by organizations in

Implementation

Require *security and privacy representatives* to be included in the *configuration change management and control process*.

SA-11(1) Static Code Analysis

Description

Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

Implementation

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11(2) Threat Modeling and Vulnerability Analyses

Description

Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the system development life cycle. Therefore, updates to threat modeling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this stage of the system development life cycle ensure that design and implementation changes have been accounted for and that vulnerabilities created because of those changes have been reviewed and mitigated.

Related Controls

PM-15, RA-3, RA-5

Implementation

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

1) Uses the following contextual information: *[Assignment: information]*;
2) Employs the following tools and methods:
   a) *[Assignment: tools and methods]*;
3) Conducts the modeling and analyses at the following level of rigor:
   a) *[Assignment: organization-defined breadth and depth of modeling and analyses]* ;
4) and (d) Produces evidence that meets the following acceptance criteria: *[Assignment: organizationdefined acceptance criteria]*.

SA-11(3) Independent Verification of Assessment Plans and Evidence

Description

Independent agents have the qualifications-including the expertise, skills, training, certifications, and experience-to verify the correct implementation of developer security and privacy assessment plans.

Related Controls

AT-3, RA-5

Implementation

TAMU-CC shall:

1) Require an independent agent satisfying *independence criteria* to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and
2) Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.

SA-11(4) Manual Code Reviews

Description

Manual code reviews are usually reserved for the critical software and firmware components of systems. Manual code reviews are effective at identifying weaknesses that require knowledge of the application's requirements or context that, in most cases, is unavailable to automated analytic tools and techniques, such as static and dynamic analysis. The benefits of manual code review include the ability to verify access control matrices against application controls and review detailed aspects of cryptographic implementations and controls.

Implementation

Require the developer of the system, system component, or system service to perform a manual code review of *[Assignment: specific code]* using the following processes, procedures, and/or techniques: *[Assignment: processes, procedures, and/or techniques]*.

SA-11(5) Penetration Testing

Description

Penetration testing is an assessment methodology in which assessors, using all available information technology product or system documentation and working under specific constraints, attempt to circumvent the implemented security and privacy features of information technology products and systems. Useful information for assessors who conduct penetration testing includes product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include white-box, gray-box, or black-box testing with analyses performed by skilled professionals who simulate adversary actions. The objective of penetration testing is to discover vulnerabilities in systems, system components, and services that result from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible. When user session information and other personally identifiable information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.

Related Controls

CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6

Implementation

Require the developer of the system, system component, or system service to perform penetration testing:

1) At the following level of rigor: *[Assignment: organization-defined breadth and depth of testing]* ; and
2) Under the following constraints: *[Assignment: constraints]*.

SA-11(6) Attack Surface Reviews

Description

Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to attacks. Attack surfaces include any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of the changes. The correction of identified flaws includes deprecation of unsafe functions.

Related Controls

SA-15

Implementation

Require the developer of the system, system component, or system service to perform attack surface reviews.

SA-11(7) Verify Scope of Testing and Evaluation

Description

Verifying that testing and evaluation provides complete coverage of required controls can be accomplished by a variety of analytic techniques ranging from informal to formal. Each of these techniques provides an increasing level of assurance that corresponds to the degree of formality of the analysis. Rigorously demonstrating control coverage at the highest levels of assurance can be

achieved using formal modeling and analysis techniques, including correlation between control implementation and corresponding test cases.

Related Controls

SA-15

Implementation

Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: *[Assignment: organization-defined breadth and depth of testing and evaluation]*.

SA-11(8) Dynamic Code Analysis

Description

Dynamic code analysis provides runtime verification of software programs using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs runtime tools to ensure that security functionality performs in the way it was designed. A type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and the assurance provided, organizations may also consider conducting code coverage analysis (i.e., checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (i.e., checking for words that are out of place in software code, such as non-English language words or derogatory terms).

Implementation

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

SA-11(9) Interactive Application Security Testing

Description

Interactive (also known as instrumentation-based) application security testing is a method of detecting vulnerabilities by observing applications as they run during testing. The use of instrumentation relies on direct measurements of the actual running applications and uses access to the code, user interaction, libraries, frameworks, backend connections, and configurations to directly measure control effectiveness. When combined with analysis techniques, interactive application security testing can identify a broad range of potential vulnerabilities and confirm control effectiveness. Instrumentation-based testing works in real time and can be used continuously throughout the system development life cycle.

Implementation

Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.

SA-12 Supply Chain Protection

Withdrawn: Incorporated into SR

SA-12(1) Acquisition Strategies / Tools / Methods

Withdrawn: Moved to SR-5

SA-12(2) Supplier Reviews

Withdrawn: Moved to SR-6

SA-12(3) Trusted Shipping and Warehousing

Withdrawn: Incorporated into SR-3

SA-12(4) Diversity of Suppliers

Withdrawn: Moved to SR-3.1

SA-12(5) Limitation of Harm

Withdrawn: Moved to SR-3.2

SA-12(6) Minimizing Procurement Time

Withdrawn: Incorporated into SR-5.1

SA-12(7) Assessments Prior to Selection / Acceptance / Update

Withdrawn: Moved to SR-5.2

SA-12(8) Use of All-source Intelligence

Withdrawn: Incorporated into RA-3.2

SA-12(9) Operations Security

Withdrawn: Moved to SR-7

SA-12(10) Validate as Genuine and Not Altered

Withdrawn: Moved to SR-4.3

SA-12(11) Penetration Testing / Analysis of Elements, Processes, and Actors

Withdrawn: Moved to SR-6.1

SA-12(12) Inter-organizational Agreements

Withdrawn: Moved to SR-8

SA-12(13) Critical Information System Components

Withdrawn: Incorporated into MA-6, RA-9

SA-12(14) Identity and Traceability

Withdrawn: Incorporated into SR-4.1, SR-4.2

SA-12(15) Processes to Address Weaknesses or Deficiencies

Withdrawn: Incorporated into SR-3

SA-13 Trustworthiness

Withdrawn: Incorporated into SA-8

SA-14 Criticality Analysis

Withdrawn: Incorporated into RA-9

SA-14(1) Critical Components with No Viable Alternative Sourcing

Withdrawn: Incorporated into SA-20

SA-15 Development Process, Standards, and Tools

Description

Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Related Controls

MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9

Implementation

TAMU-CC Shall:

1) Require the developer of the system, system component, or system service to follow a documented development process that:

a) Explicitly addresses security and privacy requirements;

b) Identifies the standards and tools used in the development process;

c) Documents the specific tool options and tool configurations used in the development process; and

d) Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

2) Review the development process, standards, tools, tool options, and tool configurations *annually* to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements of *security and privacy policies*.

SA-15(1) Quality Metrics

Description

Organizations use quality metrics to establish acceptable levels of system quality. Metrics can include quality gates, which are collections of completion criteria or sufficiency standards that represent the satisfactory execution of specific phases of the system development project. For example, a quality gate may require the elimination of all compiler warnings or a determination that such warnings have no impact on the effectiveness of required security or privacy capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. Metrics can include defining the severity thresholds of vulnerabilities in accordance with organizational risk tolerance, such as requiring no known vulnerabilities in the delivered system with a Common Vulnerability Scoring System (CVSS) severity of medium or high.

Implementation

TAMUCC Shall Require the developer of the system, system component, or system service to:

1) Define quality metrics at the beginning of the development process; and
2) Provide evidence of meeting the quality metrics*:*
    a. *Quarterly;*
    b. *program review; and*
    c. *upon delivery*.

SA-15(2) Security and Privacy Tracking Tools

Description

System development teams select and deploy security and privacy tracking tools, including vulnerability or work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with development processes.

Related Controls

SA-11

Implementation

Require the developer of the system, system component, or system service to select and employ security and privacy tracking tools for use during the development process.

SA-15(3) Criticality Analysis

Description

Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics. Criticality analysis is important for organizational systems that are designated as high value assets. High value assets can be moderate- or high-impact systems due to heightened adversarial interest

or potential adverse effects on the federal enterprise. Developer input is especially important when organizations conduct supply chain criticality analyses.

Related Controls

RA-9

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service to perform a criticality analysis:

1) At the following decision points in the system development life cycle: *[Assignment: decision points]* ; and
2) At the following level of rigor: *[Assignment: organization-defined breadth and depth of criticality analysis]*.

SA-15(4) Threat Modeling and Vulnerability Analysis

Withdrawn: Incorporated into SA-11.2

SA-15(5) Attack Surface Reduction

Description

Attack surface reduction is closely aligned with threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services. Attack surface reduction includes implementing the concept of layered defenses, applying the principles of least privilege and least functionality, applying secure software development practices, deprecating unsafe functions, reducing entry points available to unauthorized users, reducing the amount of code that executes, and eliminating application programming interfaces (APIs) that are vulnerable to attacks.

Related Controls

AC-6, CM-7, RA-3, SA-11

Implementation

Require the developer of the system, system component, or system service to reduce attack surfaces to:

1) *Eliminate Complexity;*
2) *Segment process or functions; and*
3) *Prioritize Analytics;*

SA-15(6) Continuous Improvement

Description

Developers of systems, system components, and system services consider the effectiveness and efficiency of their development processes for meeting quality objectives and addressing the security and privacy capabilities in current threat environments.

Implementation

Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.

SA-15(7) Automated Vulnerability Analysis

Description

Automated tools can be more effective at analyzing exploitable weaknesses or deficiencies in large and complex systems, prioritizing vulnerabilities by severity, and providing recommendations for risk mitigations.

Related Controls

RA-5, SA-11

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service *annually* to:

1) Perform an automated vulnerability analysis using *approved vulnerability scanner*;
2) Determine the exploitation potential for discovered vulnerabilities;
3) Determine potential risk mitigations for delivered vulnerabilities; and
4) Deliver the outputs of the tools and results of the analysis to *the Office of Information Security*.

SA-15(8) Reuse of Threat and Vulnerability Information

Description

Analysis of vulnerabilities found in similar software applications can inform potential design and implementation issues for systems under development. Similar systems or system components may exist within developer organizations. Vulnerability information is available from a variety of public and private sector sources, including the NIST National Vulnerability Database.

Implementation

Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

SA-15(9) Use of Live Data

Withdrawn: Incorporated into SA-3.2

SA-15(10) Incident Response Plan

Description

The incident response plan provided by developers may provide information not readily available to organizations and be incorporated into organizational incident response plans. Developer information may also be extremely helpful, such as when organizations respond to vulnerabilities in commercial off-the-shelf products.

Related Controls

IR-8

Implementation

Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.

SA-15(11) Archive System or Component

Description

Archiving system or system components requires the developer to retain key development artifacts, including hardware specifications, source code, object code, and relevant documentation from the development process that can provide a readily available configuration baseline for system and component upgrades or modifications.

Related Controls

CM-2

Implementation

Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.

SA-15(12) Minimize Personally Identifiable Information

Description

Organizations can minimize the risk to an individual's privacy by using techniques such as deidentification or synthetic data. Limiting the use of personally identifiable information in development and test environments helps reduce the level of privacy risk created by a system.

Related Controls

PM-25, SA-3, SA-8

Implementation

Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.

SA-16 Developer-provided Training

Description

Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Organizations can also request training materials from developers to conduct in-house training or offer self-training to

organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

Related Controls

AT-2, AT-3, PE-3, SA-4, SA-5

Implementation

Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: *[Assignment: training]*.

SA-17 Developer Security and Privacy Architecture and Design

Description

Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-8 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA-17 and PL-8 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization.

Related Controls

PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

1) Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;
2) Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and
3) Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

SA-17(1) Formal Policy Model

Description

Formal models describe specific behaviors or security and privacy policies using formal languages, thus enabling the correctness of those behaviors and policies to be formally proven. Not all components of systems can be modeled. Generally, formal specifications are scoped to the behaviors or policies of interest, such as nondiscretionary access control policies. Organizations choose the formal modeling language and approach based on the nature of the behaviors and policies to be described and the available tools.

Related Controls:

AC-3, AC-4, AC-25

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service to:

1) Produce, as an integral part of the development process, a formal policy model describing the elements of organizational security and privacy policy to be enforced; and
2) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented.

SA-17(2) Security-relevant Components

Description

The security-relevant hardware, software, and firmware represent the portion of the system, component, or service that is trusted to perform correctly to maintain required security properties.

Related Controls

AC-25, SA-5

Implementation

TAMU-CC shall Require the developer of the system, system component, or system service to:

1) Define security-relevant hardware, software, and firmware; and
2) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

SA-17(3) Formal Correspondence

Description

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, including a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to demonstrate such consistency. Consistency between the formal top-level specification and the actual implementation may require the use of an informal demonstration due to limitations on the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software,

and firmware mechanisms internal to security-relevant components include mapping registers and direct memory input and output.

Related Controls

AC-3, AC-4, AC-25, SA-4, SA-5

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service to:

1) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;
2) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;
3) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
4) Show that the formal top-level specification is an accurate description of the implemented security relevant hardware, software, and firmware; and
5) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

SA-17(4) Informal Correspondence

Description

Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that additional code or implementation detail has no impact on the behaviors or policies being modeled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Hardware, software, and firmware

mechanisms strictly internal to security-relevant hardware, software, and firmware include mapping registers and direct memory input and output.

Related Controls

AC-3, AC-4, AC-25, SA-4, SA-5

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service to:

1) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;
2) Show via *informal demonstration, convincing argument with formal methods as feasible* that the descriptive top-level specification is consistent with the formal policy model;
3) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
4) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and
5) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.

SA-17(5) Conceptually Simple Design

Description

The principle of reduced complexity states that the system design is as simple and small as possible (see SA-8(7)). A small and simple design is easier to understand and analyze and is also less prone to error (see AC-25, SA-8(13)). The principle of reduced complexity applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential. Application of the principle of

reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions and facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain. That is, simpler systems contain fewer vulnerabilities. An important benefit of reduced complexity is that it is easier to understand whether the security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex.

Related Controls

AC-25, SA-8, SC-3

Implementation

TAMU-CC Shall Require the developer of the system, system component, or system service to:

1) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and
2) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.

SA-17(6) Structure for Testing

Description

Applying the security design principles in

Related Controls

SA-5, SA-11

Implementation

Require the developer of the system, system component, or system service to structure security relevant hardware, software, and firmware to facilitate testing.

SA-17(7) Structure for Least Privilege

Description

The principle of least privilege states that each component is allocated sufficient privileges to accomplish its specified functions but no more (see SA-8(14)). Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects. First, the security impact of a failure, corruption, or misuse of the system component results in a minimized security impact. Second, the security analysis of the component is simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition. For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has a need to view the audit data that has been collected but no need to perform operations on that data. In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated upon by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality, and the access modes to the elements (e.g., read, write) are minimal.

Related Controls

AC-5, AC-6, SA-8

Implementation

Require the developer of the system, system component, or system service to structure security relevant hardware, software, and firmware to facilitate controlling access with least privilege.

SA-17(8) Orchestration

Description

Security resources that are distributed, located at different layers or in different system elements, or are implemented to support different aspects of trustworthiness can interact in unforeseen or incorrect ways. Adverse consequences can include cascading failures, interference, or coverage gaps. Coordination of the behavior of security resources (e.g., by ensuring that one patch is installed across all resources before making a configuration change that assumes that the patch is propagated) can avert such negative interactions.

Implementation

Design *critical systems* with coordinated behavior to implement the following capabilities: *[Assignment: capabilities]*.

SA-17(9) Design Diversity

Description

Design diversity is achieved by supplying the same requirements specification to multiple developers, each of whom is responsible for developing a variant of the system or system component that meets the requirements. Variants can be in software design, in hardware design, or in both hardware and a software design. Differences in the designs of the variants can result from developer experience (e.g., prior use of a design pattern), design style (e.g., when decomposing a required function into smaller tasks, determining what constitutes a separate task and how far to decompose tasks into sub-tasks), selection of libraries to incorporate into the variant, and the development environment (e.g., different design tools make some design patterns easier to

visualize). Hardware design diversity includes making different decisions about what information to keep in analog form and what information to convert to digital form, transmitting the same information at different times, and introducing delays in sampling (temporal diversity). Design diversity is commonly used to support fault tolerance.

Implementation

Use different designs for *[Assignment: critical systems]* to satisfy a common set of requirements or to provide equivalent functionality.

SA-18 Tamper Resistance and Detection

Withdrawn: Moved to SR-9

SA-18(1) Multiple Phases of System Development Life Cycle

Withdrawn: Moved to SR-9.1

SA-18(2) Inspection of Systems or Components

Withdrawn: Moved to SR-10

SA-19 Component Authenticity

Withdrawn: Moved to SR-11

SA-19(1) Anti-counterfeit Training

Withdrawn: Moved to SR-11.1

SA-19(2) Configuration Control for Component Service and Repair

Withdrawn: Moved to SR-11.2

SA-19(3) Component Disposal

Withdrawn: Moved to SR-12

SA-19(4) Anti-counterfeit Scanning

Withdrawn: Moved to SR-11.3

SA-20 Customized Development of Critical Components

Description

Organizations determine that certain system components likely cannot be trusted due to specific threats to and vulnerabilities in those components for which there are no viable security controls to adequately mitigate risk. Reimplementation or custom development of such components may satisfy requirements for higher assurance and is carried out by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to reimplement or custom develop critical system components, additional controls can be employed. Controls include enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.

Related Controls

CP-2, RA-9, SA-8

Implementation

Reimplement or custom develop the following critical system components: *[Assignment: critical system]*.

SA-21 Developer Screening

Description

Developer screening is directed at external developers. Internal developer screening is addressed by PS-3 . Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of the United States, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

Related Controls

PS-2, PS-3, PS-6, PS-7, SA-4, SR-6

Implementation

Require that the developer of a *system, systems component, or system service*:

1) Has appropriate access authorizations as determined by assigned *official government duties*; and
2) Satisfies the following additional personnel screening criteria:

[Assignment: additional personnel screening criteria].

SA-21(1) Validation of Screening

Withdrawn: Incorporated into SA-21

SA-22(1) Alternative Sources for Continued Support

Withdrawn: Incorporated into SA-22

SA-23 Specialization

Description

It is often necessary for a system or system component that supports mission-essential services or functions to be enhanced to maximize the trustworthiness of the resource. Sometimes this enhancement is done at the design level. In other instances, it is done post-design, either through modifications of the system in question or by augmenting the system with additional components. For example, supplemental authentication or non-repudiation functions may be added to the system to enhance the identity of critical resources to other resources that depend on the organization-defined resources.

Related Controls

RA-9, SA-8

Implementation

Employ *[Selection (one or more): design modification; augmentation; reconfiguration]* on *[Assignment: systems or system components]* supporting mission essential services or functions to increase the trustworthiness in those systems or components.

System and Communications Protection – 127 controls

SC-2 Separation of System and User Functionality

Description

System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. The separation of user functions from system management functions is physical or logical. Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-8 , including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14) , and SA8(18).

Related Controls

AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Separate user functionality, including user interface services, from system management functionality.

SC-2(1) Interfaces for Non-privileged Users

Description

Preventing the presentation of system management functionality at interfaces to non-privileged users ensures that system administration options, including administrator privileges, are not available to the general user population. Restricting user access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information. One potential solution is to withhold system administration options until users establish sessions with administrator privileges.

Related Controls

AC-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent the presentation of system management functionality at interfaces to non-privileged users.

SC-2(2) Disassociability

Implementation

Store state information from applications and software separately.

Description

If a system is compromised, storing applications and software separately from state information about users' interactions with an application may better protect individuals' privacy.

SC-3 Security Function Isolation

Description

Security functions are isolated from nonsecurity functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to and protects the integrity of the hardware, software, and firmware that perform system security functions. Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code. Systems can restrict access to security functions using access control mechanisms and by implementing least privilege capabilities. While the ideal is for all code within the defined security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions as an exception. The isolation of security functions from nonsecurity functions can be achieved by applying the systems security engineering design principles in SA-8 , including SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14) , and SA-8(18).

Related Controls

AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Isolate security functions from nonsecurity functions.

SC-3(1) Hardware Separation

Description

Hardware separation mechanisms include hardware ring architectures that are implemented within microprocessors and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ hardware separation mechanisms to implement security function isolation.

SC-3(2) Access and Flow Control Functions

Description

Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include auditing, intrusion detection, and malicious code protection functions.

Implementation

Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.

SC-3(3) Minimize Nonsecurity Functionality

Description

Where it is not feasible to achieve strict isolation of nonsecurity functions from security functions, it is necessary to take actions to minimize nonsecurity-relevant functions within the security function boundary. Nonsecurity functions contained within the isolation boundary are considered security-relevant because errors or malicious code in the software can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems that provide information security are of minimal size and complexity. Minimizing the number of nonsecurity functions in the security-relevant system components allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing the nonsecurity functions within the isolation boundaries, the amount of code that is trusted to enforce security policies is significantly reduced, thus contributing to understandability.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.

SC-3(4) Module Coupling and Cohesiveness

Description

The reduction of inter-module interactions helps to constrain security functions and manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between functions within a module. Best practices in software engineering and systems security engineering rely on layering, minimization, and modular decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

SC-3(5) Layered Structures

Description

The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) enables the isolation of security functions and the management of complexity.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

SC-4 Information in Shared System Resources

Description

Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection.

Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related Controls

AC-3, AC-4, SA-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent unauthorized and unintended information transfer via shared system resources.

SC-4(1) Security Levels

Withdrawn: Incorporated into SC-4

SC-4(2) Multilevel or Periods Processing

Description

Changes in processing levels can occur during multilevel or periods processing with information at different classification levels or security categories. It can also occur during serial reuse of hardware components at different classification levels. Organization-defined procedures can include approved sanitization processes for electronically stored information.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent unauthorized information transfer via shared resources in accordance with *[Assignment: procedures]* when system processing explicitly switches between different information classification levels or security categories.

SC-5(1) Restrict Ability to Attack Other Systems

Description

Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial-ofservice attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: *[Assignment: denial-of-service attacks]*.

SC-5(2) Capacity, Bandwidth, and Redundancy

Description

Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.

SC-5(3) Detection and Monitoring

Description

Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles. Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems

to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

Related Controls

CA-7, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: *[Assignment: monitoring tools]* ; and
2) Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: *[Assignment: system resources]*.

SC-6 Resource Availability

Description

Priority protection prevents lower-priority processes from delaying or interfering with the system that services higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources.

Related Controls

SC-5

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Protect the availability of resources by allocating *[Assignment: resources]* by *[Selection (one or more): priority; quota; _[Assignment: controls]_]*.

SC-7(1) Physically Separated Subnetworks

Withdrawn: Incorporated into SC-7

SC-7(2) Public Access

Withdrawn: Incorporated into SC-7

SC-7(3) Access Points

Description

Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Limit the number of external network connections to the system.

SC-7(4) External Telecommunications Services

Description

External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See

Related Controls

AC-3, SC-8, SC-20, SC-21, SC-22

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Implement a managed interface for each external telecommunication service;

2) Establish a traffic flow policy for each managed interface;
3) Protect the confidentiality and integrity of the information being transmitted across each interface;
4) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
5) Review exceptions to the traffic flow policy *annually* and remove exceptions that are no longer supported by an explicit mission or business need;
6) Prevent unauthorized exchange of control plane traffic with external networks;
7) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
8) Filter unauthorized control plane traffic from external networks.

SC-7(5) Deny by Default - Allow by Exception

Description

Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Deny network communications traffic by default and allow network communications traffic by exception.

SC-7(6) Response to Recognized Failures

Withdrawn: Incorporated into SC-7.18

SC-7(7) Split Tunneling for Remote Devices

Description

Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using *[Assignment: safeguards]*.

SC-7(8) Route Traffic to Authenticated Proxy Servers

Description

External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services. Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of virtual private networks (VPNs) and create the potential for

Related Controls

AC-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Route *internal communications traffic* to e*xternal networks* through authenticated proxy servers at managed interfaces.

SC-7(9) Restrict Threatening Outgoing Communications Traffic

Description

Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out within the system at managed interfaces. Extrusion detection includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code. Organizations have criteria to determine, update, and manage identified threats related to extrusion detection.

Related Controls

AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Detect and deny outgoing communications traffic posing a threat to external systems; and

2) Audit the identity of internal users associated with denied communications.

SC-7(10) Prevent Exfiltration

Description

Prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected, call backs to command and control centers, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools. Devices that enforce strict adherence to protocol formats include deep packet inspection firewalls and Extensible Markup Language (XML) gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices that operate at the network or transport layers. The prevention of exfiltration is similar to data loss prevention or data leakage prevention and is closely associated with cross-domain solutions and system guards that enforce information flow requirements.

Related Controls

AC-2, CA-8, SI-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Prevent the exfiltration of information; and
2) Conduct exfiltration tests *annually*.

SC-7(11) Restrict Incoming Communications Traffic

Description

General source address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs. Strong authentication of network addresses is not possible without the use of explicit security protocols, and thus, addresses can often be spoofed. Further, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.

Related Controls

AC-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Only allow incoming communications from *authorized sources* to be routed to *authorized destinations*.

SC-7(12) Host-based Protection

Description

Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement *host-based boundary protection mechanisms* at *[Assignment: system components]*.

SC-7(13) Isolation of Security Tools, Mechanisms, and Support Components

Description

Physically separate subnetworks with managed interfaces are useful in isolating computer network defenses from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques employed by organizations.

Related Controls

SC-2, SC-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Isolate *information security tools, mechanisms, and support components* from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7(14) Protect Against Unauthorized Physical Connections

Description

Systems that operate at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls that enforce limited authorized access to these items.

Related Controls

PE-4, PE-19

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Protect against unauthorized physical connections at *[Assignment: managed interfaces]*.

SC-7(15) Networked Privileged Accesses

Description

Privileged access provides greater accessibility to system functions, including security functions. Adversaries attempt to gain privileged access to systems through remote access to cause adverse mission or business impacts, such as by exfiltrating information or bringing down a critical system capability. Routing networked, privileged access requests through a dedicated, managed interface further restricts privileged access for increased access control and auditing.

Related Controls

AC-2, AC-3, AU-2, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

SC-7(16) Prevent Discovery of System Components

Description

Preventing the discovery of system components representing a managed interface helps protect network addresses of those components from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery and require prior knowledge for access. Preventing the discovery of components and devices can be accomplished by not publishing network addresses, using network address translation, or not entering the addresses in domain name systems. Another prevention technique is to periodically change network addresses.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent the discovery of specific system components that represent a managed interface.

SC-7(17) Automated Enforcement of Protocol Formats

Description

System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components verify adherence to protocol formats and specifications at the

application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.

Related Controls

SC-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Enforce adherence to protocol formats.

SC-7(18) Fail Secure

Description

Fail secure is a condition achieved by employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as demilitarized zones). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices nor can failures permit unauthorized information releases.

Related Controls

CP-2, CP-12, SC-24

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

SC-7(19) Block Communication from Non-organizationally Configured Hosts

Description

Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Block inbound and outbound communications traffic between *communication clients* that are independently configured by end users and external service providers.

SC-7(20) Dynamic Isolation and Segregation

Description

The capability to dynamically isolate certain internal system components is useful when it is necessary to partition or separate system components of questionable origin from components that possess greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide the capability to dynamically isolate *system components* from other system components.

SC-7(21) Isolation of System Components

Description

Organizations can isolate system components that perform different mission or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components. Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to more effectively control information flows between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber-attacks and errors. The degree of isolation varies depending upon the mechanisms chosen. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into physically separate networks or subnetworks; cross-domain

devices that separate subnetworks; virtualization techniques; and the encryption of information flows among system components using distinct encryption keys.

Related Controls

CA-9

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ boundary protection mechanisms to isolate *system components* supporting *missions and/or business functions*.

SC-7(22) Separate Subnets for Connecting to Different Security Domains

Description

The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains that contain information with different security categories or classification levels.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement separate network addresses to connect to systems in different security domains.

SC-7(23) Disable Sender Feedback on Protocol Validation Failure

Description

Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information that would otherwise be unavailable.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Disable feedback to senders on protocol format validation failure.

SC-7(24) Personally Identifiable Information

Description

Managing the processing of personally identifiable information is an important aspect of protecting an individual’s privacy. Applying, monitoring for, and documenting exceptions to processing rules ensure that personally identifiable information is processed only in accordance with established privacy requirements.

Related Controls

PT-2, SI-15

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

For systems that process personally identifiable information TAMU-CC Shall:

1) Apply the following processing rules to data elements of personally identifiable information: *[Assignment: processing rules]*;
2) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
3) Document each processing exception; and
4) Review and remove exceptions that are no longer supported.

SC-7(25) Unclassified National Security System Connections

Description

A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified national security systems and external networks.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit the direct connection of *unclassified national security system* to an external network without the use of *boundary protection device*.

SC-7(26) Classified National Security System Connections

Description

A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface or cross-domain systems) provide information flow enforcement from systems to external networks.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit the direct connection of a classified national security system to an external network without the use of *boundary protection device*.

SC-7(27) Unclassified Non-national Security System Connections

Description

A direct connection is a dedicated physical or virtual connection between two or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified non-national security systems and external networks.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit the direct connection of *unclassified, non-national security system* to an external network without the use of *boundary protection device*.

SC-7(28) Connections to Public Networks

Description

A direct connection is a dedicated physical or virtual connection between two or more systems. A public network is a network accessible to the public, including the Internet and organizational extranets with public access.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Prohibit the direct connection of *[Assignment: system]* to a public network.

SC-7(29) Separate Subnets to Isolate Functions

Description

Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command and control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in the trustworthiness of critical system functions.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement *[Selection: physically; logically]* separate subnetworks to isolate the following critical system components and functions: *[Assignment: critical system components and functions]*.

SC-8(1) Cryptographic Protection

Description

Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and IPSec. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to *[Selection (one or more): prevent unauthorized disclosure of information; detect changes to information]* during transmission.

SC-8(2) Pre- and Post-transmission Handling

Description

Information can be unintentionally or maliciously disclosed or modified during preparation for transmission or during reception, including during aggregation, at protocol transformation points, and during packing and unpacking. Such unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Maintain the *confidentiality and integrity* of information during preparation for transmission and during reception.

SC-8(3) Cryptographic Protection for Message Externals

Description

Cryptographic protection for message externals addresses protection from the unauthorized disclosure of information. Message externals include message headers and routing information. Cryptographic protection prevents the exploitation of message externals and applies to internal and external networks or links that may be visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in clear text (i.e., unencrypted) because the information is not identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical controls include protected distribution systems.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to protect message externals unless otherwise protected by *alternative physical controls*.

SC-8(4) Conceal or Randomize Communications

Description

Concealing or randomizing communication patterns addresses protection from unauthorized disclosure of information. Communication patterns include frequency, periods, predictability, and amount. Changes to communications patterns can reveal information with intelligence value, especially when combined with other available information related to the mission and business functions of the organization. Concealing or randomizing communications prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed, or random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical controls include protected distribution systems.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by *alternative physical controls*.

SC-8(5) Protected Distribution System

Description

The purpose of a protected distribution system is to deter, detect, and/or make difficult physical access to the communication lines that carry national security information.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement *[Assignment: protected distribution system]* to *[Selection (one or more): prevent unauthorized disclosure of information; detect changes to information]* during transmission.

SC-9 Transmission Confidentiality

Withdrawn: Incorporated into SC-8

SC-10 Network Disconnect

Description

Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Related Controls

AC-17, SC-23

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Terminate the network connection associated with a communications session at the end of the session or after *[Assignment: time period]* of inactivity.

SC-11 Trusted Path

Description

Trusted paths are mechanisms by which users can communicate (using input devices such as keyboards) directly with the security functions of systems with the requisite assurance to support security policies. Trusted path mechanisms can only be activated by users or the security functions of organizational systems. User responses that occur via trusted paths are protected from modification by and disclosure to untrusted applications. Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users, including during system logons. The original implementations of trusted paths employed an outof-band signal to initiate the path, such as using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used (e.g., the <CTRL> + <ALT> + <DEL> keys). Such key combinations, however, are platform-specific and may not provide a trusted path implementation in every case. The enforcement of trusted communications paths is provided by a specific implementation that meets the reference monitor concept.

Related Controls

AC-16, AC-25, SC-12, SC-23

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

a. Provide a *[Selection: physically; logically]* isolated trusted communications path for communications between the user and the trusted components of the system; and

b. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: *[Assignment: security functions]*.

SC-11(1) Irrefutable Communications Path

Description

An irrefutable communications path permits the system to initiate a trusted path, which necessitates that the user can unmistakably recognize the source of the communication as a trusted system component. For example, the trusted path may appear in an area of the display that other applications cannot access or be based on the presence of an identifier that cannot be spoofed.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

(a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and (b) Initiate the trusted communications path for communications between the *[Assignment: security functions]* of the system and the user.

SC-12(1) Availability

Description

Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Maintain availability of information in the event of the loss of cryptographic keys by users.

SC-12(2) Symmetric Keys

Description

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Produce, control, and distribute symmetric cryptographic keys using *[Selection: NIST FIPSvalidated; NSA-approved]* key management technology and processes.

SC-12(3) Asymmetric Keys

Description

[SP 800-56A], [SP 800-56B], and [SP 800-56C] provide guidance on cryptographic

key establishment schemes and key derivation methods. [SP 800-57-1], [SP 800-57-2], and

[SP 800-57-3] provide guidance on cryptographic key management.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Produce, control, and distribute asymmetric cryptographic keys using [Selection: NSAapproved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoDissued Medium Hardware Assurance PKI certificates and hardware security tokens that
protect the user's private key; certificates issued in accordance with organization-defined requirements].

SC-12(4) PKI Certificates

Withdrawn: Incorporated into SC-12.3

SC-12(5) PKI Certificates / Hardware Tokens

Withdrawn: Incorporated into SC-12.3

SC-12(6) Physical Control of Keys

Description

For organizations that use external service providers (e.g., cloud service or data center providers), physical control of cryptographic keys provides additional assurance that information stored by such external providers is not subject to unauthorized disclosure or modification.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.

SC-13(1) Fips-validated Cryptography

Withdrawn: Incorporated into SC-13

SC-13(2) Nsa-approved Cryptography

Withdrawn: Incorporated into SC-13

SC-13(3) Individuals Without Formal Access Approvals

Withdrawn: Incorporated into SC-13

SC-13(4) Digital Signatures

Withdrawn: Incorporated into SC-13

SC-14 Public Access Protections

Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10

SC-15(1) Physical or Logical Disconnect

Description

Failing to disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures. Disconnect from collaborative computing devices can be manual or automatic.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide *[Selection (one or more): physical; logical]* disconnect of collaborative computing devices in a manner that supports ease of use.

SC-15(2) Blocking Inbound and Outbound Communications Traffic

Withdrawn: Incorporated into SC-7

SC-15(3) Disabling and Removal in Secure Work Areas

Description

Failing to disable or remove collaborative computing devices and applications from systems or system components can result in compromises of information, including eavesdropping on conversations. A Sensitive Compartmented Information Facility (SCIF) is an example of a secure work area.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Disable or remove collaborative computing devices and applications from *[Assignment: systems or system components]* in *[Assignment: secure work areas]*.

SC-15(4) Explicitly Indicate Current Participants

Description

Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide an explicit indication of current participants in *[Assignment: online meetings and teleconferences]*.

SC-16 Transmission of Security and Privacy Attributes

Description

Security and privacy attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components. Attributes are abstractions that represent the basic properties or characteristics of an entity with respect to protecting information or the management of personally identifiable information. Attributes are typically associated with internal data structures, including records, buffers, and files within the system. Security and privacy attributes are used to implement access control and information flow control policies; reflect special dissemination, management, or distribution instructions, including permitted uses of personally identifiable information; or support other aspects of the information security and privacy policies. Privacy attributes may be used independently or in conjunction with security attributes.

Related Controls

AC-3, AC-4, AC-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Associate *[Assignment: organization-defined security and privacy attributes]* with information exchanged between systems and between system components.

SC-16(1) Integrity Verification

Description

Part of verifying the integrity of transmitted information is ensuring that security and privacy attributes that are associated with such information have not been modified in an unauthorized manner. Unauthorized modification of security or privacy attributes can result in a loss of integrity for transmitted information.

Related Controls

AU-10, SC-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Verify the integrity of transmitted security and privacy attributes.

SC-16(2) Anti-spoofing Mechanisms

Description

Some attack vectors operate by altering the security attributes of an information system to intentionally and maliciously implement an insufficient level of security within the system. The alteration of attributes leads organizations to believe that a greater number of security functions are in place and operational than have actually been implemented.

Related Controls

SI-3, SI-4, SI-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.

SC-16(3) Cryptographic Binding

Description

Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of such information.

Related Controls

AC-16, SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement *mechanisms or techniques* to bind security and privacy attributes to transmitted information.

SC-17 Public Key Infrastructure Certificates

Description

Public key infrastructure (PKI) certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Related Controls

AU-10, IA-5, SC-12

Applicability

Implementation

a. Issue public key certificates under an *[Assignment: certificate policy]* or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-18 Mobile Code

Description

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Related Controls

AU-2, AU-12, CM-2, CM-6, SI-3

Applicability

Implementation

TAMU-CC Shall:

1) Define acceptable and unacceptable mobile code and mobile code technologies; and

2) Authorize, monitor, and control the use of mobile code within the system.

SC-18(1) Identify Unacceptable Code and Take Corrective Actions

Description

Corrective actions when unacceptable mobile code is detected include blocking, quarantine, or alerting administrators. Blocking includes preventing the transmission of word processing files with embedded macros when such macros have been determined to be unacceptable mobile code.

Applicability

Implementation

Identify *[Assignment: unacceptable mobile code]* and take *[Assignment: corrective actions]*.

SC-18(2) Acquisition, Development, and Use

Description

None.

Applicability

Implementation

Verify that the acquisition, development, and use of mobile code to be deployed in the system meets *[Assignment: mobile code requirements]*.

SC-18(3) Prevent Downloading and Execution

Description

None.

Applicability

Implementation

Prevent the download and execution of *[Assignment: unacceptable mobile code]*.

SC-18(4) Prevent Automatic Execution

Description

Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing the automatic execution of mobile code includes disabling auto-execute features on system components that employ portable storage devices, such as compact discs, digital versatile discs, and universal serial bus devices.

Applicability

Implementation

Prevent the automatic execution of mobile code in *[Assignment: software applications]* and enforce *[Assignment: actions]* prior to executing the code.

SC-18(5) Allow Execution Only in Confined Environments

Description

Permitting the execution of mobile code only in confined virtual machine environments helps prevent the introduction of malicious code into other systems and system components.

Related Controls

SC-44, SI-7

Applicability

Implementation

Allow execution of permitted mobile code only in confined virtual machine environments.

SC-19 Voice Over Internet Protocol

Withdrawn: === Control Technology-specific; addressed as any other technology or protocol.

SC-20(1) Child Subspaces

Withdrawn: Incorporated into SC-20

SC-20(2) Data Origin and Integrity

Description

None.

Applicability

Implementation

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

SC-21(1) *Data* Origin and Integrity

Withdrawn: Incorporated into SC-21

SC-23 Session Authenticity

Description

Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against

Related Controls

AU-10, SC-8, SC-10, SC-11

Applicability

Implementation

Protect the authenticity of communications sessions.

SC-23(1) Invalidate Session Identifiers at Logout

Description

Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Invalidate session identifiers upon user logout or other session termination.

SC-23(2) User-initiated Logouts and Message Displays

Withdrawn: Incorporated into AC-12.1

SC-23(3) Unique System-generated Session Identifiers

Description

Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Related Controls

AC-10, SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Generate a unique session identifier for each session with *[Assignment: randomness requirements]* and recognize only session identifiers that are system-generated.

SC-23(4) Unique Session Identifiers with Randomization

Withdrawn: Incorporated into SC-23.3

SC-23(5) Allowed Certificate Authorities

Description

Reliance on certificate authorities for the establishment of secure sessions includes the use of Transport Layer Security (TLS) certificates. These certificates, after verification by their respective

certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Only allow the use of *[Assignment: certificated authorities]* for verification of the establishment of protected sessions.

SC-24 Fail in Known State

Description

Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode with less disruption of mission and business processes.

Related Controls

CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Fail to a *[Assignment: known system state]* for the following failures on the indicated components while preserving *[Assignment: system state information]* in failure: *[Assignment: types of system failures on system components]*.

SC-25 Thin Nodes

Description

The deployment of system components with minimal functionality reduces the need to secure every endpoint and may reduce the exposure of information, systems, and services to attacks.
Reduced or minimal functionality includes diskless nodes and thin client technologies.

Related Controls

SC-30, SC-44

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ minimal functionality and information storage on the following system components: *[Assignment: system components]*.

SC-26 Decoys

Description

Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational mission and business functions. Use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems. Depending on the specific usage of the decoy, consultation with the Office of the General Counsel before deployment may be needed.

Related Controls

RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

SC-26(1) Detection of Malicious Code

Withdrawn: Incorporated into SC-35

SC-27 Platform-independent Applications

Description

Platforms are combinations of hardware, firmware, and software components used to execute software applications. Platforms include operating systems, the underlying computer architectures, or both. Platform-independent applications are applications with the capability to execute on multiple platforms. Such applications promote portability and reconstitution on different platforms. Application portability and the ability to reconstitute on different platforms increase the availability of mission-essential functions within organizations in situations where systems with specific operating systems are under attack.

Related Controls

SC-29

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Include within organizational systems the following platform independent applications: *[Assignment: platform-independent applications]*.

SC-28 Protection of Information at Rest

Description

Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

Related Controls

AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC13, SC-34, SI-3, SI-7, SI-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Protect the *[Selection (one or more): confidentiality; integrity]* of the following information at rest: *[Assignment: information at rest]*.

SC-28(1) Cryptographic Protection

Description

The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Related Controls

AC-19, SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on *[Assignment: system components or media]*: *[Assignment: information]*.

SC-28(2) Offline Storage

Description

Removing organizational information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to offline storage in lieu of protecting such information in online storage.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Remove the following information from online storage and store offline in a secure location: *[Assignment: information]*.

SC-28(3) Cryptographic Keys

Description

A Trusted Platform Module (TPM) is an example of a hardware-protected data store that can be used to protect cryptographic keys.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Provide protected storage for cryptographic keys *[Selection: _[Assignment: safeguards]_; hardware-protected key store]*.

SC-29 Heterogeneity

Description

Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be effective against other system components, thus further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead that could ultimately lead to mistakes and unauthorized configurations.

Related Controls

AU-9, PL-8, SC-27, SC-30, SR-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ a diverse set of information technologies for the following system components in the implementation of the system: *[Assignment: system components]*.

SC-29(1) Virtualization Techniques

Description

While frequent changes to operating systems and applications can pose significant configuration management challenges, the changes can result in an increased work factor for adversaries to conduct successful attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems or applications, provides virtual changes that impede attacker success while reducing configuration management efforts. Virtualization techniques can assist in isolating untrustworthy software or software of dubious provenance into confined execution environments.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed *[Assignment: frequency]*.

SC-30 Concealment and Misdirection

Description

Concealment and misdirection techniques can significantly reduce the targeting capabilities of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. The increased use of concealment and misdirection techniques and methodsincluding randomness, uncertainty, and virtualization-may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment and misdirection techniques may provide additional time to perform core mission and business functions. The implementation of concealment and misdirection techniques may add to the complexity and management overhead required for the system.

Related Controls

AC-6, SC-25, SC-26, SC-29, SC-44, SI-14

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ the following concealment and misdirection techniques for *[Assignment: systems]* at *[Assignment: time periods]* to confuse and mislead adversaries: *[Assignment: concealment and misdirection techniques]*.

SC-30(1) Virtualization Techniques

Withdrawn: Incorporated into SC-29.1

SC-30(2) Randomness

Description

Randomness introduces increased levels of uncertainty for adversaries regarding the actions that organizations take to defend their systems against attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations that support critical missions or business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques that involve randomness include performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating roles and responsibilities of organizational personnel.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ *[Assignment: techniques]* to introduce randomness into organizational operations and assets.

SC-30(3) Change Processing and Storage Locations

Description

Adversaries target critical mission and business functions and the systems that support those mission and business functions while also trying to minimize the exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational systems targeted by adversaries make such systems more susceptible to attacks with less adversary cost and effort to be successful. Changing processing and storage locations (also referred to as moving target defense) addresses the advanced persistent threat using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the system components (i.e., processing, storage) that support critical mission and business functions. Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty into the targeting activities of adversaries. The targeting uncertainty increases the work factor of adversaries and makes compromises or breaches of the organizational systems more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose certain aspects of their tradecraft while attempting to locate critical organizational resources.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Change the location of *[Assignment: processing and/or storage] [Selection: _[Assignment: time frequency]_; random time intervals]*].

SC-30(4) Misleading Information

Description

Employing misleading information is intended to confuse potential adversaries regarding the nature and extent of controls deployed by organizations. Thus, adversaries may employ incorrect and ineffective attack techniques. One technique for misleading adversaries is for organizations to place misleading information regarding the specific controls deployed in external systems that are known to be targeted by adversaries. Another technique is the use of deception nets that mimic actual aspects of organizational systems but use, for example, out-of-date software configurations.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ realistic, but misleading information in *[Assignment: system components]* about its security state or posture.

SC-30(5) Concealment of System Components

Description

By hiding, disguising, or concealing critical system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means to hide, disguise, or conceal system components include the configuration of routers or the use of encryption or virtualization techniques.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ the following techniques to hide or conceal *[Assignment: system components]*: *[Assignment: techniques]*.

SC-31 Covert Channel Analysis

Description

Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, such as in the case of systems that contain export-controlled information and have connections to external networks (i.e., networks that are not controlled by organizations). Covert channel analysis is also useful for multilevel secure systems, multiple security level systems, and cross-domain systems.

Related Controls

AC-3, AC-4, SA-8, SI-11

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert *[Selection (one or more): storage; timing]* channels; and

b. Estimate the maximum bandwidth of those channels.

SC-31(1) Test Covert Channels for Exploitability

Description

None.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Test a subset of the identified covert channels to determine the channels that are exploitable.

SC-31(2) Maximum Bandwidth

Description

The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Reduce the maximum bandwidth for identified covert *[Selection (one or more): storage; timing]* channels to *[Assignment: values]*.

SC-31(3) Measure Bandwidth in Operational Environments

Description

Measuring covert channel bandwidth in specified operational environments helps organizations determine how much information can be covertly leaked before such leakage adversely affects mission or business functions. Covert channel bandwidth may be significantly different when measured in settings that are independent of the specific environments of operation, including laboratories or system development environments.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Measure the bandwidth of *[Assignment: subset of identified covert channels]* in the operational environment of the system.

SC-32 System Partitioning

Description

System partitioning is part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components. Physical separation options include physically distinct components in separate racks in the same room, critical components in separate rooms, and geographical separation of critical components. Security categorization can guide the selection of candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

Related Controls

AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Partition the system into *[Assignment: system components]* residing in separate *[Selection: physical; logical]* domains or environments based on *[Assignment: circumstances for the physical or logical separation of components]*.

SC-32(1) Separate Physical Domains for Privileged Functions

Description

Privileged functions that operate in a single physical domain may represent a single point of failure if that domain becomes compromised or experiences a denial of service.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Partition privileged functions into separate physical domains.

SC-33 Transmission Preparation Integrity

Withdrawn: Incorporated into SC-8

SC-34 Non-modifiable Executable Programs

Description

The operating environment for a system contains the code that hosts applications, including operating systems, executives, or virtual machine monitors (i.e., hypervisors). It can also include certain applications that run directly on hardware platforms. Hardware-enforced, read-only media include Compact Disc-Recordable (CD-R) and Digital Versatile Disc-Recordable (DVD-R) disk drives as well as one-time, programmable, read-only memory. The use of non-modifiable storage

ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable, read-only memory can be accepted as read-only media provided that integrity can be adequately protected from the point of initial writing to the insertion of the memory into the system, and there are reliable hardware protections against reprogramming the memory while installed in organizational systems.

Related Controls

AC-3, SI-7, SI-14

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

For *[Assignment: system components]* , load and execute: a. The operating environment from hardware-enforced, read-only media; and b. The following applications from hardware-enforced, read-only media: *[Assignment: applications]*.

SC-34(1) No Writable Storage

Description

Disallowing writeable storage eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated system components. The restriction applies to fixed and removable storage, with the latter being addressed either directly or as specific restrictions imposed through access controls for mobile devices.

Related Controls

AC-19, MP-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ *[Assignment: system components]* with no writeable storage that is persistent across component restart or power on/off.

SC-34(2) Integrity Protection on Read-only Media

Description

Controls prevent the substitution of media into systems or the reprogramming of programmable read-only media prior to installation into the systems. Integrity protection controls include a combination of prevention, detection, and response.

Related Controls

CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.

SC-34(3) Hardware-based Protection

Withdrawn: Moved to SC-51

SC-35 External Malicious Code Identification

Description

External malicious code identification differs from decoys in SC-26 in that the components actively probe networks, including the Internet, in search of malicious code contained on external websites. Like decoys, the use of external malicious code identification techniques requires some supporting isolation measures to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems. Virtualization is a common technique for achieving such isolation.

Related Controls

SC-7, SC-26, SC-44, SI-3, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Include system components that proactively seek to identify network-based malicious code or malicious websites.

SC-36 Distributed Processing and Storage

Description

Distributing processing and storage across multiple physical locations or logical domains provides a degree of redundancy or overlap for organizations. The redundancy and overlap increase the work factor of adversaries to adversely impact organizational operations, assets, and individuals. The use of distributed processing and storage does not assume a single primary processing or storage location. Therefore, it allows for parallel processing and storage.

Related Controls

CP-6, CP-7, PL-8, SC-32

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Distribute the following processing and storage components across multiple *[Selection: physical locations; logical domains]*: *[Assignment: organization-defined processing and storage components]*.

SC-36(1) Polling Techniques

Description

Distributed processing and/or storage may be used to reduce opportunities for adversaries to compromise the confidentiality, integrity, or availability of organizational information and systems. However, the distribution of processing and storage components does not prevent adversaries from compromising one or more of the components. Polling compares the processing results and/or storage content from the distributed components and subsequently votes on the outcomes. Polling identifies potential faults, compromises, or errors in the distributed processing and storage components.

Related Controls

SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

(a) Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: *[Assignment: distributed processing and storage components]* ; and (b) Take the following actions in response to identified faults, errors, or compromises: *[Assignment: actions]*.

SC-36(2) Synchronization

Description

SC-36 and CP-9(6) require the duplication of systems or system components in distributed locations. The synchronization of duplicated and redundant services and data helps to ensure that information contained in the distributed locations can be used in the mission or business functions of organizations, as needed.

Related Controls

CP-9

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Synchronize the following duplicate systems or system components: *[Assignment: duplicate systems or system components]*.

SC-37 Out-of-band Channels

Description

Out-of-band channels include local, non-network accesses to systems; network paths physically separate from network paths used for operational traffic; or non-electronic paths, such as the U.S. Postal Service. The use of out-of-band channels is contrasted with the use of in-band channels (i.e., the same channels) that carry routine operational traffic. Out-of-band channels do not have the

same vulnerability or exposure as in-band channels. Therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-ofband channels. Organizations may employ out-of-band channels in the delivery or transmission of organizational items, including authenticators and credentials; cryptographic key management information; system and data backups; configuration management changes for hardware, firmware, or software; security updates; maintenance information; and malicious code protection updates.

Related Controls

AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ the following out-of-band channels for the physical delivery or electronic transmission of *[Assignment: information, system components, or devices]* to *[Assignment: individuals or systems]*: *[Assignment: out-of-band channels]*.

SC-37(1) Ensure Delivery and Transmission

Description

Techniques employed by organizations to ensure that only designated systems or individuals receive certain information, system components, or devices include sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ *[Assignment: controls]* to ensure that only *[Assignment: individuals or systems]* receive the following information, system components, or devices: *[Assignment: information, system components, or devices]*.

SC-38 Operations Security

Description

Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and the application of appropriate countermeasures. OPSEC controls are applied to organizational systems and the environments in which those systems operate. OPSEC controls protect the confidentiality of information, including limiting the sharing of information with suppliers, potential suppliers, and other non-organizational elements and individuals. Information critical to organizational mission and business functions includes user identities, element uses, suppliers, supply chain processes, functional requirements, security requirements, system design specifications, testing and evaluation protocols, and security control implementation details.

Related Controls

CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ the following operations security controls to protect key organizational information throughout the system development life cycle: *[Assignment: operations security controls]*.

SC-39(1) Hardware Separation

Description

Hardware-based separation of system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Hardware separation mechanisms include hardware memory management.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement hardware separation mechanisms to facilitate process isolation.

SC-39(2) Separate Execution Domain Per Thread

Description

None.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Maintain a separate execution domain for each thread in *[Assignment: multi-threaded processing]*.

SC-40 Wireless Link Protection

Description

Wireless link protection applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof system users. Protection of wireless links reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement wireless link protections to the extent necessary to meet organizational security requirements.

Related Controls

AC-18, SC-5

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Protect external and internal *[Assignment: organization-defined wireless links]* from the following signal parameter attacks: *[Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks]*.

SC-40(1) Electromagnetic Interference

Description

The implementation of cryptographic mechanisms for electromagnetic interference protects systems against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The implementation of cryptographic mechanisms may also coincidentally mitigate the effects of unintentional jamming due to interference from legitimate transmitters that share the same spectrum. Mission requirements, projected threats, concept of operations, and laws, executive orders, directives, regulations, policies, and standards determine levels of wireless link availability, cryptography needed, and performance.

Related Controls

PE-21, SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms that achieve *[Assignment: level of protection]* against the effects of intentional electromagnetic interference.

SC-40(2) Reduce Detection Potential

Description

The implementation of cryptographic mechanisms to reduce detection potential is used for covert communications and to protect wireless transmitters from geo-location. It also ensures that the spread spectrum waveforms used to achieve a low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable laws, executive orders, directives, regulations, policies, and standards determine the levels to which wireless links are undetectable.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to reduce the detection potential of wireless links to *[Assignment: level of reduction]*.

SC-40(3) Imitative or Manipulative Communications Deception

Description

The implementation of cryptographic mechanisms to identify and reject imitative or manipulative communications ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based on signal parameters alone.

Related Controls

SC-12, SC-13, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

SC-40(4) Signal Parameter Identification

Description

The implementation of cryptographic mechanisms to prevent the identification of wireless transmitters protects against the unique identification of wireless transmitters for the purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. It also provides anonymity when required. Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission or user identification.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement cryptographic mechanisms to prevent the identification of *[Assignment: wireless transmitters]* by using the transmitter signal parameters.

SC-41 Port and I/O Device Access

Description

Connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE 1394). Input/output (I/O) devices include compact disc and digital versatile disc drives. Disabling or

removing such connection ports and I/O devices helps prevent the exfiltration of information from systems and the introduction of malicious code from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action.

Related Controls

AC-20, MP-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

[Selection: physically; logically] disable or remove *[Assignment: connection ports or input/output devices]* on the following systems or system components: *[Assignment: systems or system components]*.

SC-42 Sensor Capability and Data

Description

Sensor capability and data applies to types of systems or system components characterized as mobile devices, such as cellular telephones, smart phones, and tablets. Mobile devices often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include microphones, cameras, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for

adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the movements of an individual. Organizations may prohibit individuals from bringing cellular telephones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations are taking place.

Related Controls

SC-15

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

a. Prohibit *[Selection (one or more): the use of devices possessing _[Assignment: environmental sensing capabilities]_ in _[Assignment: facilities, areas, or systems]_; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: _[Assignment: exceptions where remote activation of sensors is allowed]_]* ; and

b. Provide an explicit indication of sensor use to *[Assignment: group of users]*.

SC-42(1) Reporting to Authorized Individuals or Roles

Description

In situations where sensors are activated by authorized individuals, it is still possible that the data or information collected by the sensors will be sent to unauthorized entities.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Verify that the system is configured so that data or information collected by the *[Assignment: sensors]* is only reported to authorized individuals or roles.

SC-42(2) Authorized Use

Description

Information collected by sensors for a specific authorized purpose could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track the movements of individuals. Measures to mitigate such activities include additional training to help ensure that authorized individuals do not abuse their authority and, in the case where sensor data is maintained by external parties, contractual restrictions on the use of such data.

Related Controls

PT-2

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ the following measures so that data or information collected by *[Assignment: sensors]* is only used for authorized purposes: *[Assignment: measures]*.

SC-42(3) Prohibit Use of Devices

Withdrawn: Incorporated into SC-42

SC-42(4) Notice of Collection

Description

Awareness that organizational sensors are collecting data enables individuals to more effectively engage in managing their privacy. Measures can include conventional written notices and sensor configurations that make individuals directly or indirectly aware through other devices that the sensor is collecting information. The usability and efficacy of the notice are important considerations.

Related Controls

PT-1, PT-4, PT-5

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by *[Assignment: sensors]*: *[Assignment: measures]*.

SC-42(5) Collection Minimization

Description

Although policies to control for authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy risk at the system entry point and mitigates the risk of policy control failures. Sensor configurations include the obscuring of human features, such as blurring or pixelating flesh tones.

Related Controls

SA-8, SI-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ *[Assignment: sensors]* that are configured to minimize the collection of information about individuals that is not needed.

SC-43 Usage Restrictions

Description

Usage restrictions apply to all system components including but not limited to mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.

Related Controls

AC-18, AC-19, CM-6, SC-7, SC-18

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

a. Establish usage restrictions and implementation guidelines for the following system components: *[Assignment: components]* ; and

b. Authorize, monitor, and control the use of such components within the system.

SC-44 Detonation Chambers

Description

Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

Related Controls

SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Employ a detonation chamber capability within *[Assignment: system, system component, or location]*.

SC-45 System Time Synchronization

Description

Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and timeof-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result without properly synchronized clocks within and between systems and system components. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities-such as access control and identification and authentication-depending on the nature of the mechanisms used to support the capabilities.

Related Controls

AC-3, AU-8, IA-2, IA-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Synchronize system clocks within and between systems and system components.

SC-45(1) Synchronization with Authoritative Time Source

Description

Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

(a) Compare the internal system clocks *[Assignment: frequency]* with *[Assignment: authoritative time source]* ; and (b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than *[Assignment: time period]*.

SC-45(2) Secondary Authoritative Time Source

Description

It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

(a) Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and (b) Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

SC-46 Cross Domain Policy Enforcement

Description

For logical policy enforcement mechanisms, organizations avoid creating a logical path between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation afforded by the physical implementation of policy enforcement to preclude the presence of logical covert channels penetrating the security domain may be needed. Contact

Related Controls

AC-4, SC-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement a policy enforcement mechanism *[Selection: physically; logically]* between the physical and/or network interfaces for the connecting security domains.

SC-47 Alternate Communications Paths

Description

An incident, whether adversarial- or nonadversarial-based, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. To compound the problem, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communications path incident, can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communications paths for command and control purposes, including designating alternative decision makers if primary decision makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization's ability to continue to operate and take appropriate actions during an incident.

Related Controls

CP-2, CP-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Establish *[Assignment: alternate communication paths]* for system operations organizational command and control.

SC-48 Sensor Relocation

Description

Adversaries may take various paths and use different approaches as they move laterally through an organization (including its systems) to reach their target or as they attempt to exfiltrate information from the organization. The organization often only has a limited set of monitoring and detection capabilities, and they may be focused on the critical or likely infiltration or exfiltration paths. By using communications paths that the organization typically does not monitor, the adversary can increase its chances of achieving its desired goals. By relocating its sensors or monitoring capabilities to new locations, the organization can impede the adversary's ability to achieve its goals. The relocation of the sensors or monitoring capabilities might be done based on threat information that the organization has acquired or randomly to confuse the adversary and make its lateral transition through the system or organization more challenging.

Related Controls

AU-2, SC-7, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Relocate *[Assignment: sensors and monitoring capabilities]* to *[Assignment: locations]* under the following conditions or circumstances: *[Assignment: conditions or circumstances]*.

SC-48(1) Dynamic Relocation of Sensors or Monitoring Capabilities

Description

None.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Dynamically relocate *[Assignment: sensors and monitoring capabilities]* to *[Assignment: locations]* under the following conditions or circumstances: *[Assignment: conditions or circumstances]*.

SC-49 Hardware-enforced Separation and Policy Enforcement

Description

System owners may require additional strength of mechanism and robustness to ensure domain separation and policy enforcement for specific types of threats and environments of operation. Hardware-enforced separation and policy enforcement provide greater strength of mechanism than software-enforced separation and policy enforcement.

Related Controls

AC-4, SA-8, SC-50

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement hardware-enforced separation and policy enforcement mechanisms between *[Assignment: security domains]*.

SC-50 Software-enforced Separation and Policy Enforcement

Description

System owners may require additional strength of mechanism to ensure domain separation and policy enforcement for specific types of threats and environments of operation.

Related Controls

AC-3, AC-4, SA-8, SC-2, SC-3, SC-49

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

Implement software-enforced separation and policy enforcement mechanisms between *[Assignment: security domains]*.

SC-51 Hardware-based Protection

Description

None.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information resources owners and custodians.

Implementation

a. Employ hardware-based, write-protect for *[Assignment: system firmware components]* ; and

b. Implement specific procedures for *[Assignment: authorized individuals]* to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.

SI-2(1) Central Management – 95 controls

Withdrawn: Incorporated into PL-9

SI-2(2) Automated Flaw Remediation Status

Description

Automated mechanisms can track and determine the status of known flaws for system components.

Related Controls

CA-7, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Determine if system components have applicable security-relevant software and firmware updates installed using *automated mechanisms monthly*.

SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions

Description

Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Measure the time between flaw identification and flaw remediation; and
2) Establish the following benchmarks for taking corrective actions: *[Assignment: benchmarks]*.

SI-2(4) Automated Patch Management Tools

Description

Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ automated patch management tools to facilitate flaw remediation to the following system components: *[Assignment: components]*.

SI-2(5) Automatic Software and Firmware Updates

Description

Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Install *security-relevant software and firmware updates* automatically to *system components*.

SI-2(6) Removal of Previous Versions of Software and Firmware

Description

Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Remove previous versions of *software and firmware components* after updated versions have been installed.

SI-3(1) Central Management

Withdrawn: Incorporated into PL-9

SI-3(2) Automatic Updates

Withdrawn: Incorporated into SI-3

SI-3(3) Non-privileged Users

Withdrawn: Incorporated into AC-6.10

SI-3(4) Updates Only by Privileged Users

Description

Protection mechanisms for malicious code are typically categorized as security-related software and, as such, are only updated by organizational personnel with appropriate access privileges.

Related Controls

CM-5

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Update malicious code protection mechanisms only when directed by a privileged user.

SI-3(5) Portable Storage Devices

Withdrawn: Incorporated into MP-7

SI-3(6) Testing and Verification

Description

None.

Related Controls

CA-2, CA-7, RA-5

Implementation

TAMU-CC Shall:

1) Test malicious code protection mechanisms *annually* by introducing known benign code into the system; and
2) Verify that the detection of the code and the associated incident reporting occur.

SI-3(7) Nonsignature-based Detection

Withdrawn: Incorporated into SI-3

SI-3(8) Detect Unauthorized Commands

Description

Detecting unauthorized commands can be applied to critical interfaces other than kernel-based interfaces, including interfaces with virtual machines and privileged applications. Unauthorized operating system commands include commands for kernel functions from system processes that are not trusted to initiate such commands as well as commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can also define hardware components by component type, component, component location in the network, or a combination

thereof. Organizations may select different actions for different types, classes, or instances of malicious commands.

Related Controls

AU-2, AU-6, AU-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1. Detect the following unauthorized operating system commands through the kernel application programming interface on *system hardware components*: *[Assignment: unauthorized operating system commands]* ; and
2. *[Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command]*.

SI-3(9) Authenticate Remote Commands

Withdrawn: Moved to AC-17.10

SI-3(10) Malicious Code Analysis

Description

The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code

facilitates effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by employing reverse engineering techniques or by monitoring the behavior of executing code.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: *[Assignment: tools and techniques]* ; and
2) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

SI-4(1) System-wide Intrusion Detection System

Description

Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

SI-4(2) Automated Tools and Mechanisms for Real-time Analysis

Description

Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessment and make determinations that are in alignment with their privacy program plan.

Related Controls

PM-23, PM-25

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ automated tools and mechanisms to support near real-time analysis of events.

SI-4(3) Automated Tool and Mechanism Integration

Description

Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination.

Related Controls

PM-23, PM-25

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.

SI-4(4) Inbound and Outbound Communications Traffic

Description

Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of

information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
2) Monitor inbound and outbound communications traffic *[Assignment: organization-defined frequency]* for *unusual or unauthorized activities or conditions*.

SI-4(5) System-generated Alerts

Description

Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related Controls

AU-4, AU-5, PE-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Alert *the Office of Information Security* when the following system-generated indications of compromise or potential compromise occur: *[Assignment: compromise indicators]*.

SI-4(6) Restrict Non-privileged Users

Withdrawn: Incorporated into AC-6.10

SI-4(7) Automated Response to Suspicious Events

Description

Least-disruptive actions include initiating requests for human responses.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Notify *the Office of Information Security* of detected suspicious events; and
2) Take the following actions upon detection: *[Assignment: least-disruptive actions]*.

SI-4(8) Protection of Monitoring Information

Withdrawn: Incorporated into SI-4

SI-4(9) Testing of Monitoring Tools and Mechanisms

Description

Testing intrusion-monitoring tools and mechanisms is necessary to ensure that the tools and mechanisms are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency and depth of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Test intrusion-monitoring tools and mechanisms *annually*.

SI-4(10) Visibility of Encrypted Communications

Description

Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Make provisions so that *encrypted communications traffic* is visible to *system monitoring tools and mechanisms*.

SI-4(11) Analyze Communications Traffic Anomalies

Description

Organization-defined interior points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Analyze outbound communications traffic at the external interfaces to the system and selected *[Assignment: interior points]* to discover anomalies.

SI-4(12) Automated Organization-generated Alerts

Description

Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, senior agency information security officer, senior agency official for privacy, system security officers, or privacy officers. Automated organization generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-4(5) focus on information sources that are internal to the systems, such as audit records.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Alert *the Office of information Security* using *automated mechanisms* when the following indications of inappropriate or unusual activities with security or privacy implications occur: *[Assignment: activities that trigger alerts]*.

SI-4(13) Analyze Traffic and Event Patterns

Description

Identifying and understanding common communications traffic and event patterns help organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Analyze communications traffic and event patterns for the system;
2) Develop profiles representing common traffic and event patterns; and
3) Use the traffic and event profiles in tuning system-monitoring devices.

SI-4(14) Wireless Intrusion Detection

Description

Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including the conduct of thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

Related Controls

AC-18, IA-3

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

SI-4(15) Wireless to Wireline Communications

Description

Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given the greater facility of unauthorized network access via wireless access points compared to unauthorized wired network access from within the physical boundaries of the system,

additional monitoring of transitioning traffic between wireless and wired networks may be necessary to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps to ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.

Related Controls

AC-18

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

SI-4(16) Correlate Monitoring Information

Description

Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation-including malicious code protection software, host monitoring, and network monitoring-can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Related Controls

AU-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Correlate information from monitoring tools and mechanisms employed throughout the system.

SI-4(17) Integrated Situational Awareness

Description

Correlating monitoring information from a more diverse set of information sources helps to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out such attacks. In contrast to SI-4(16) , which correlates the various cyber monitoring information, integrated situational awareness is intended to correlate monitoring beyond the cyber domain. Correlation of monitoring information from multiple activities may help reveal attacks on organizations that are operating across multiple attack vectors.

Related Controls

AU-16, PE-6, SR-2, SR-4, SR-6

Implementation

Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

SI-4(18) Analyze Traffic and Covert Exfiltration

Description

Organization-defined interior points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: *[Assignment: interior points]*.

SI-4(19) Risk for Individuals

Description

Indications of increased risk from individuals can be obtained from different sources, including personnel records, intelligence agencies, law enforcement organizations, and other sources. The monitoring of individuals is coordinated with the management, legal, security, privacy, and human resource officials who conduct such monitoring. Monitoring is conducted in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement *additional monitoring* of individuals who have been identified by *[Assignment: sources]* as posing an increased level of risk.

SI-4(20) Privileged Users

Description

Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.

Related Controls

AC-18

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement the following additional monitoring of privileged users: *[Assignment: additional monitoring]*.

SI-4(21) Probationary Periods

Description

During probationary periods, employees do not have permanent employment status within organizations. Without such status or access to information that is resident on the system, additional monitoring can help identify any potentially malicious activity or inappropriate behavior.

Related Controls

AC-18

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement the following additional monitoring of individuals during *the probationary period*: *[Assignment: additional monitoring]*.

SI-4(22) Unauthorized Network Services

Description

Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

Related Controls

CM-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Detect network services that have not been authorized or approved by *[Assignment: authorization or approval processes]*; and
2) *[Selection (one or more): audit; alert [Assignment: personnel or roles]]* when detected.

SI-4(23) Host-based Devices

Description

Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook

computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

Related Controls

AC-18, AC-19

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement the following host-based monitoring mechanisms at *[Assignment: system components]*: *[Assignment: host-based monitoring mechanisms]*.

SI-4(24) Indicators of Compromise

Description

Indicators of compromise (IOC) are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffic include Universal Resource Locator or protocol elements that indicate malicious code command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Threat indicators, signatures, tactics, techniques, procedures, and other indicators of compromise may be available via government and non-government cooperatives, including the Forum of Incident Response and Security Teams, the United States

Computer Emergency Readiness Team, the Defense Industrial Base Cybersecurity Information Sharing Program, and the CERT Coordination Center.

Related Controls

AC-18

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Discover, collect, and distribute to *[Assignment: personnel or roles]*, indicators of compromise provided by *[Assignment: sources]*.

SI-4(25) Optimize Network Traffic Analysis

Description

Encrypted traffic, asymmetric routing architectures, capacity and latency limitations, and transitioning from older to newer technologies (e.g., IPv4 to IPv6 network protocol transition) may result in blind spots for organizations when analyzing network traffic. Collecting, decrypting, preprocessing, and distributing only relevant traffic to monitoring devices can streamline the efficiency and use of devices and optimize traffic analysis.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.

SI-5(1) Automated Alerts and Advisories

Description

The significant number of changes to organizational systems and environments of operation requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational mission and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the three levels related to the management of risk, including the governance level, mission and business process level, and the information system level.

Applicability

Security alerts, advisories, and directives are the responsibility of the Chief Information Security and Privacy Officer (CISPO).

Implementation

Broadcast security alert and advisory information throughout the organization using *automated mechanisms*.

SI-6 Security and Privacy Function Verification

Description

Transitional states for systems include system startup, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected and are approved by the senior agency official for privacy or that privacy attributes are applied or used as expected.

Related Controls

CA-7, CM-4, CM-6, SI-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Verify the correct operation of *[Assignment: organization-defined security and privacy functions]*;

2) Perform the verification of the functions specified in SI-6a *[Selection (one or more): [Assignment: system transitional states]; upon command by user with appropriate privilege; [Assignment: frequency]]*;

3) Alert *the Office of Information Security* to failed security and privacy verification tests; and

4) *[Selection (one or more): shut the system down; restart the system; [Assignment: alternative action(s)]]* when anomalies are discovered.

SI-6(1) Notification of Failed Security Tests

Withdrawn: Incorporated into SI-6

SI-6(2) Automation Support for Distributed Testing

Description

The use of automated mechanisms to support the management of distributed function testing helps to ensure the integrity, timeliness, completeness, and efficacy of such testing.

Related Controls

SI-2

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement automated mechanisms to support the management of distributed security and privacy function testing.

SI-6(3) Report Verification Results

Description

Organizational personnel with potential interest in the results of the verification of security and privacy functions include systems security officers, senior agency information security officers, and senior agency officials for privacy.

Related Controls

SI-4, SR-4, SR-5

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Report the results of security and privacy function verification to *the Office of Information Security*.

SI-7 Software, Firmware, and Information Integrity

Description

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms-including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools-can automatically monitor the integrity of systems and hosted applications.

Related Controls

AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: *[Assignment: organization-defined software, firmware, and information]* ; and

2) Take the following actions when unauthorized changes to the software, firmware, and information are detected: *[Assignment: organization-defined actions]*.

SI-7(1) Integrity Checks

Description

Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Perform an integrity check of *[Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at _[Assignment: organization-defined transitional states or security-relevant events]_; _[Assignment: organization-defined frequency]_]*.

SI-7(2) Automated Notifications of Integrity Violations

Description

The employment of automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential to effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior agency information security official, senior agency official for privacy, system administrators, software developers, systems integrators, information security officers, and privacy officers.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ automated tools that provide notification to *the Office of Information Security* upon discovering discrepancies during integrity verification.

SI-7(3) Centrally Managed Integrity Tools

Description

Centrally managed integrity verification tools provides greater consistency in the application of such tools and can facilitate more comprehensive coverage of integrity verification actions.

Related Controls

AU-3, SI-2, SI-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ centrally managed integrity verification tools.

SI-7(4) Tamper-evident Packaging

Withdrawn: Incorporated into SR-9

SI-7(5) Automated Response to Integrity Violations

Description

Organizations may define different integrity-checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Automatically *[Selection (one or more): shut down the system; restart the system; implement _[Assignment: controls]_]* when integrity violations are discovered.

SI-7(6) Cryptographic Protection

Description

Cryptographic mechanisms used to protect integrity include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

SI-7(7) Integration of Detection and Response

Description

Integrating detection and response helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important for being able to identify and discern adversary actions over an extended time period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related Controls

AU-2, AU-6, IR-4, IR-5, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: *[Assignment: changes]*.

SI-7(8) Auditing Capability for Significant Events

Description

Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

Related Controls

AU-2, AU-6, AU-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: *[Selection (one or more): generate an audit record; alert current user; alert _[Assignment: personnel or roles]_; _[Assignment: other actions]]*.

SI-7(9) Verify Boot Process

Description

Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.

Related Controls

SI-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information

resources owners and custodians.

Implementation

Verify the integrity of the boot process of the following system components: *[Assignment: system components]*.

SI-7(10) Protection of Boot Firmware

Description

Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.

Related Controls

SI-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement the following mechanisms to protect the integrity of boot firmware in *[Assignment: system components]*: *[Assignment: mechanisms]*.

SI-7(11) Confined Environments with Limited Privileges

Withdrawn: Moved to CM-7.6

SI-7(12) Integrity Verification

Description

Organizations verify the integrity of user-installed software prior to execution to reduce the likelihood of executing malicious code or programs that contains errors from unauthorized modifications. Organizations consider the practicality of approaches to verifying software integrity, including the availability of trustworthy checksums from software developers and vendors.

Related Controls

CM-11

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Require that the integrity of user-installed software be verified prior to execution.

SI-7(13) Code Execution in Protected Environments

Withdrawn: Moved to CM-7.7

SI-7(14) Binary or Machine Executable Code

Withdrawn: Moved to CM-7.8

SI-7(15) Code Authentication

Description

Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms also consider cryptographic key management solutions.

Related Controls

CM-5, SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: *[Assignment: software or firmware components]*.

SI-7(16) Time Limit on Process Execution Without Supervision

Description

Placing a time limit on process execution without supervision is intended to apply to processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes timers on operating systems, automated responses, and manual oversight and response when system process anomalies occur.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Prohibit processes from executing without supervision for more than *[Assignment: time period]*.

SI-7(17) Runtime Application Self-protection

Description

Runtime application self-protection employs runtime instrumentation to detect and block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections such as guards and firewalls which can only detect and block attacks by using network information without contextual awareness. Runtime application self-protection technology can reduce the susceptibility of software to attacks by monitoring its inputs and blocking those inputs that could allow attacks. It can also help protect the runtime environment from unwanted changes and tampering. When a threat is detected, runtime application self-protection technology can prevent exploitation and take other actions (e.g., sending a warning message to the user, terminating the user's session,

terminating the application, or sending an alert to organizational personnel). Runtime application self-protection solutions can be deployed in either a monitor or protection mode.

Related Controls

SI-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement *controls* for application self-protection at runtime.

SI-8 Spam Protection

Description

System entry and exit points include firewalls, remote-access servers, electronic mail servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web accesses. Spam protection mechanisms include signature definitions.

Related Controls

PL-9, SC-5, SC-7, SC-38, SI-3, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
2) Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8(1) Central Management

Withdrawn: Incorporated into PL-9

SI-8(2) Automatic Updates

Description

Using automated mechanisms to update spam protection mechanisms helps to ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Automatically update spam protection mechanisms *[Assignment: frequency]*.

SI-8(3) Continuous Learning Capability

Description

Learning mechanisms include Bayesian filters that respond to user inputs that identify specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.

SI-9 Information Input Restrictions

Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6

SI-10(1) Manual Override Capability

Description

In certain situations, such as during events that are defined in contingency plans, a manual override capability for input validation may be needed. Manual overrides are used only in limited circumstances and with the inputs defined by the organization.

Related Controls

AC-3, AU-2, AU-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Provide a manual override capability for input validation of the following information inputs: *[Assignment: information inputs]*;
2) Restrict the use of the manual override capability to only *authorized individuals* ; and
3) Audit the use of the manual override capability.

SI-10(2) Review and Resolve Errors

Description

Resolution of input validation errors includes correcting systemic causes of errors and resubmitting transactions with corrected input. Input validation errors are those related to the information inputs defined by the organization in the base control (SI-10).

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Review and resolve input validation errors within *[Assignment: organization-defined time period]*.

SI-10(3) Predictable Behavior

Description

A common vulnerability in organizational systems is unpredictable behavior when invalid inputs are received. Verification of system predictability helps ensure that the system behaves as expected when invalid inputs are received. This occurs by specifying system responses that allow the system to transition to known states without adverse, unintended side effects. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

SI-10(4) Timing Interactions

Description

In addressing invalid system inputs received across protocol interfaces, timing interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols in the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to noise or collisions on the link. If TCP makes a congestion response, it takes the wrong action in response to a collision event. Adversaries may be able to use what appear to be acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information

resources owners and custodians.

Implementation

Account for timing interactions among system components in determining appropriate responses for invalid inputs.

SI-10(5) Restrict Inputs to Trusted Sources and Approved Formats

Description

Restricting the use of inputs to trusted sources and in trusted formats applies the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity. The information inputs are those defined by the organization in the base control (SI-10).

Related Controls

AC-3, AC-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Restrict the use of information inputs to *trusted sources* and/or *formats*.

SI-10(6) Injection Prevention

Description

Untrusted data injections may be prevented using a parameterized interface or output escaping (output encoding). Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter's parser whether data is trusted. Prevention of untrusted data injections are with respect to the information inputs defined by the organization in the base control (SI-10).

Related Controls

AC-3, AC-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Prevent untrusted data injections.

SI-11 Error Handling

Description

Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and

personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related Controls

AU-2, AU-3, SC-31, SI-2, SI-15

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

2) Reveal error messages only to *[Assignment: personnel or roles]*.

SI-12(1) Limit Personally Identifiable Information Elements

Description

Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system. The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

Related Controls

PM-25

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: *[Assignment: elements of personally identifiable information]*.

SI-12(2) Minimize Personally Identifiable Information in Testing, Training, and Research

Description

Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining the techniques to use and when to use them.

Related Controls

PM-22, PM-25, SI-19

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: *[Assignment: organization-defined techniques]*.

SI-12(3) Information Disposal

Description

Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Use the following techniques to dispose of, destroy, or erase information following the retention period: *[Assignment: organization-defined techniques]*.

SI-13 Predictable Failure Prevention

Description

While MTTF is primarily a reliability issue, predictable failure prevention is intended to address potential failures of system components that provide security capabilities. Failure rates reflect installation-specific consideration rather than the industry-average. Organizations define the criteria for the substitution of system components based on the MTTF value with consideration for the potential harm from component failures. The transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capabilities. The preservation of system state variables is also critical to help ensure a successful transfer process. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

Related Controls

CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Determine mean time to failure (MTTF) for the following system components in specific environments of operation: *[Assignment: system components]* ; and

2) Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: *[Assignment: mean time to failure (MTTF) substitution criteria]*.

SI-13(1) Transferring Component Responsibilities

Description

Transferring primary system component responsibilities to other substitute components prior to primary component failure is important to reduce the risk of degraded or debilitated mission or business functions. Making such transfers based on a percentage of mean time to failure allows organizations to be proactive based on their risk tolerance. However, the premature replacement of system components can result in the increased cost of system operations.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Take system components out of service by transferring component responsibilities to substitute components no later than *[Assignment: fraction or percentage]* of mean time to failure.

SI-13(2) Time Limit on Process Execution Without Supervision

Withdrawn: Incorporated into SI-7.16

SI-13(3) Manual Transfer Between Components

Description

For example, if the MTTF for a system component is 100 days and the MTTF percentage defined by the organization is 90 percent, the manual transfer would occur after 90 days.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Manually initiate transfers between active and standby system components when the use of the active component reaches *[Assignment: percentage]* of the mean time to failure.

SI-13(4) Standby Component Installation and Notification

Description

Automatic or manual transfer of components from standby to active mode can occur upon the detection of component failures.

Implementation

If system component failures are detected TAMU-CC Shall:

1) Ensure that the standby components are successfully and transparently installed within *[Assignment: time period]* ; and
2) *[Selection (one or more): activate _[Assignment: alarm]_; automatically shut down the system; _[Assignment: action]_]*.

SI-13(5) Failover Capability

Description

Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes incorporating mirrored system operations at alternate processing sites or periodic data mirroring at regular intervals defined by the recovery time periods of organizations.

Related Controls

CP-6, CP-7, CP-9

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Provide *[Selection: real-time; near real-time] [Assignment: failover capability]* for the system.

SI-14 Non-persistence

Description

Implementation of non-persistent components and services mitigates risk from advanced persistent threats (APTs) by reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a trusted, known state computing resource for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems or operating environments. Since the APT is a high-end, sophisticated threat with regard to capability, intent, and targeting, organizations assume that over an extended period, a percentage of attacks will be successful. Non-persistent system components and services are activated as required using protected information and terminated periodically or at the end of sessions. Non-persistence increases the work factor of adversaries attempting to compromise or breach organizational systems. Nonpersistence can be achieved by refreshing system components, periodically reimaging components, or using a variety of common virtualization techniques. Non-persistent services can be implemented by using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent). The benefit of periodic refreshes of system components and services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the system unstable. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

Related Controls

SC-30, SC-34, SI-21

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement non-persistent *system components and services* that are initiated in a known state and terminated *upon end of session of use*.

SI-14(1) Refresh from Trusted Sources

Description

Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Obtain software and data employed during system component and service refreshes from the following trusted sources: *[Assignment: trusted sources]*.

SI-14(2) Non-persistent Information

Description

Retaining information longer than is needed makes the information a potential target for advanced adversaries searching for high value assets to compromise through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, unnecessary retention provides advanced adversaries information that can assist in their reconnaissance and lateral movement through the system.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) *[Selection: refresh _[Assignment: information]_ _[Assignment: frequency]_; generate_[Assignment: information]_ on demand]* ; and
2) Delete information when no longer needed.

SI-14(3) Non-persistent Connectivity

Description

Persistent connections to systems can provide advanced adversaries with paths to move laterally through systems and potentially position themselves closer to high value assets. Limiting the availability of such connections impedes the adversary’s ability to move freely through organizational systems.

Related Controls

SC-10

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Establish connections to the system on demand and terminate connections after *[Selection: completion of a request; a period of non-use]*.

SI-15 Information Output Filtering

Description

Certain types of attacks, including SQL injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications. Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behavior has been discovered.

Related Controls

SI-3, SI-4, SI-11

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: *[Assignment: software programs and/or applications]*.

SI-16 Memory Protection

Description

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism.

Related Controls

AC-25, SC-3, SI-7

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Implement controls to protect the system memory from unauthorized code execution.

SI-17 Fail-safe Procedures

Description

Failure conditions include the loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps may include doing nothing, reestablishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

Related Controls

CP-12, CP-13, SC-24, SI-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information

resources owners and custodians.

Implementation

Implement the indicated fail-safe procedures when the indicated failures occur: *[Assignment: organization-defined list of failure conditions and associated fail-safe procedures]*.

SI-18 Personally Identifiable Information Quality Operations

Description

Personally identifiable information quality operations include the steps that organizations take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information. Personally identifiable information quality operations include editing and validating addresses as they are collected or entered into systems using automated address verification look-up application programming interfaces. Checking personally identifiable information quality includes the tracking of updates or changes to data over time, which enables organizations to know how and what personally identifiable information was changed should erroneous information be identified. The measures taken to protect personally identifiable information quality are based on the nature and context of the personally identifiable information, how it is to be used, how it was obtained, and the potential de-identification methods employed. The measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals covered under federal programs may be more comprehensive than the measures used to validate personally identifiable information used for less sensitive purposes.

Related Controls

PM-22, PM-24, PT-2, SI-4

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle *[Assignment: organization-defined frequency]*; and

2) Correct or delete inaccurate or outdated personally identifiable information.

SI-18(1) Automation Support

Description

The use of automated mechanisms to improve data quality may inadvertently create privacy risks. Automated tools may connect to external or otherwise unrelated systems, and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their privacy impact assessments and make determinations that are in alignment with their privacy program plans. As data is obtained and used across the information life cycle, it is important to confirm the accuracy and relevance of personally identifiable information. Automated mechanisms can augment existing data quality processes and procedures and enable an organization to better identify and manage personally identifiable information in large-scale systems. For example, automated tools can greatly improve efforts to consistently normalize data or identify malformed data. Automated tools can also be used to improve the auditing of data and detect errors that may incorrectly alter personally identifiable

information or incorrectly associate such information with the wrong individual. Automated capabilities backstop processes and procedures at-scale and enable more fine grained detection and correction of data quality errors.

Related Controls

PM-18, RA-8

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using *automated mechanisms*.

SI-18(2) Data Tags

Description

Data tagging personally identifiable information includes tags that note processing permissions, authority to process, de-identification, impact level, information life cycle stage, and retention or last updated dates. Employing data tags for personally identifiable information can support the use of automation tools to correct or delete relevant personally identifiable information.

Related Controls

AC-3, AC-16, SC-16

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.

SI-18(3) Collection

Description

Individuals or their designated representatives can be sources of correct personally identifiable information. Organizations consider contextual factors that may incentivize individuals to provide correct data versus false data. Additional steps may be necessary to validate collected information based on the nature and context of the personally identifiable information, how it is to be used, and how it was obtained. The measures taken to validate the accuracy of personally identifiable information used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than the measures taken to validate less sensitive personally identifiable information.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Collect personally identifiable information directly from the individual.

SI-18(4) Individual Requests

Description

Inaccurate personally identifiable information maintained by organizations may cause problems for individuals, especially in those business functions where inaccurate information may result in inappropriate decisions or the denial of benefits and services to individuals. Even correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of an organization maintaining the information. Organizations use discretion when determining if personally identifiable information is to be corrected or deleted based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies. Organizational personnel consult with the senior agency official for privacy and legal counsel regarding appropriate instances of correction or deletion.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Correct or delete personally identifiable information upon request by individuals or their designated representatives.

SI-18(5) Notice of Correction or Deletion

Description

When personally identifiable information is corrected or deleted, organizations take steps to ensure that all authorized recipients of such information, and the individual with whom the information is associated or their designated representatives, are informed of the corrected or deleted information.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Notify *recipients* and individuals that the personally identifiable information has been corrected or deleted.

SI-19 De-identification

Description

De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. Many datasets contain information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Personally identifiable information is removed from datasets by trained individuals when such information is not (or no longer) necessary to satisfy the requirements

envisioned for the data. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies. Reidentification is a residual risk with de-identified data. Re-identification attacks can vary, including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time support the management of this residual risk.

Related Controls

MP-6, PM-22, PM-23, PM-24, RA-2, SI-12

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

a. Remove the following elements of personally identifiable information from datasets: *[Assignment: elements]*; and

b. Evaluate *[Assignment: frequency]* for effectiveness of de-identification.

SI-19(1) Collection

Description

If a data source contains personally identifiable information but the information will not be used, the dataset can be de-identified when it is created by not collecting the data elements that contain the

personally identifiable information. For example, if an organization does not intend to use the social security number of an applicant, then application forms do not ask for a social security number.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

De-identify the dataset upon collection by not collecting personally identifiable information.

SI-19(2) Archiving

Description

Datasets can be archived for many reasons. The envisioned purposes for the archived dataset are specified, and if personally identifiable information elements are not required, the elements are not archived. For example, social security numbers may have been collected for record linkage, but the archived dataset may include the required elements from the linked records. In this case, it is not necessary to archive the social security numbers.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.

SI-19(3) Release

Description

Prior to releasing a dataset, a data custodian considers the intended uses of the dataset and determines if it is necessary to release personally identifiable information. If the personally identifiable information is not necessary, the information can be removed using de-identification techniques.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.

SI-19(4) Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers

Description

There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is

transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption
Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.

SI-19(5) Statistical Disclosure Implementation

Description

Many types of statistical analyses can result in the disclosure of information about individuals even if only summary information is provided. For example, if a school that publishes a monthly table with the number of minority students enrolled, reports that it has 10-19 such students in January, and subsequently reports that it has 20-29 such students in March, then it can be inferred that the student who enrolled in February was a minority.

Implementation

Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.

SI-19(6) Differential Privacy

Description

The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual). In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine-learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Nondeterministic noise can include adding small, random values to the results of mathematical operations in dataset analysis.

Related Controls

SC-12, SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.

SI-19(7) Validated Algorithms and Software

Description

Algorithms that appear to remove personally identifiable information from a dataset may in fact leave information that is personally identifiable or data that is re-identifiable. Software that is claimed to implement a validated algorithm may contain bugs or implement a different algorithm. Software may de-identify one type of data, such as integers, but not de-identify another type of data, such as floating-point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Perform de-identification using validated algorithms and software that is validated to implement the algorithms.

SI-19(8) Motivated Intruder

Description

A motivated intruder test is a test in which an individual or group takes a data release and specified resources and attempts to re-identify one or more individuals in the de-identified dataset. Such tests specify the amount of inside knowledge, computational resources, financial resources, data, and skills that intruders possess to conduct the tests. A motivated intruder test can determine if the de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient. However, the test alone cannot prove that deidentification is sufficient.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.

SI-20 Tainting

Description

Many cyber-attacks target organizational information, or information that the organization holds on behalf of other entities (e.g., personally identifiable information), and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system that is in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any packets it includes potentially contain malicious code, and that the unauthorized entity may have potentially obtained a copy of the database. Another tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open-source analysis. Finally, an active tainting approach can include embedding software in the data that is able to

Related Controls

AU-13

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: *[Assignment: systems or system components]*.

SI-21 Information Refresh

Description

Retaining information for longer than it is needed makes it an increasingly valuable and enticing target for adversaries. Keeping information available for the minimum period of time needed to support organizational missions or business functions reduces the opportunity for adversaries to compromise, capture, and exfiltrate that information.

Related Controls

SI-14

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Refresh *information* at *[Assignment: frequencies]* or generate the information on demand and delete the information when no longer needed.

SI-22 Information Diversity

Description

Actions taken by a system service or a function are often driven by the information it receives. Corruption, fabrication, modification, or deletion of that information could impact the ability of the service function to properly carry out its intended actions. By having multiple sources of input, the service or function can continue operation if one source is corrupted or no longer available. It is possible that the alternative sources of information may be less precise or less accurate than the primary source of information. But having such sub-optimal information sources may still provide a sufficient level of quality that the essential service or function can be carried out, even in a degraded or debilitated manner.

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

TAMU-CC Shall:

1) Identify the following alternative sources of information for *essential functions and services*: *[Assignment: alternative information sources]* ; and

2) Use an alternative information source for the execution of essential functions or services on *systems or system components* when the primary source of information is corrupted or unavailable.

SI-23 Information Fragmentation

Description

One objective of the advanced persistent threat is to exfiltrate valuable information. Once exfiltrated, there is generally no way for the organization to recover the lost information. Therefore, organizations may consider dividing the information into disparate elements and distributing those elements across multiple systems or system components and locations. Such actions will increase the adversary's work factor to capture and exfiltrate the desired information and, in so doing, increase the probability of detection. The fragmentation of information impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation is dictated by the impact or classification level (and value) of the information, threat intelligence information received, and whether data tainting is used (i.e., data tainting-derived information about the exfiltration of some information could result in the fragmentation of the remaining information).

Applicability

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this Control are implemented. The intended audience for this Control includes, but is not limited to, all information
resources owners and custodians.

Implementation

Based on *[Assignment: circumstances] TAMU-CC Shall*:

1) Fragment the following information: *[Assignment: information]* ; and
2) Distribute the fragmented information across the following systems or system components: *[Assignment: systems or system components]*.