Access Control (AC) – 16 controls

AC-1 Access Control Policy and Procedures

AC-2 Account Management

AC-2(7) Privileged User Accounts

AC-3 Access Enforcement

AC-3(7) Role-based Access Control

AC-5 Separation of Duties

AC-6 Least Privilege

AC-7 Unsuccessful Login Attempts

AC-8 System Use Notification

AC-11 Session Lock

AC-14 Permitted Actions Without Identification or Authentication

AC-17 Remote Access

AC-18 Wireless Access

AC-19 Access Control for Mobile Devices

AC-20 Use of External Information Systems

AC-22 Publicly Accessible Content

Awareness and Training (AT) - 4 controls

AT-1 Awareness and Training Policy and Procedures

AT-2 Security Awareness Training

AT-3 Role-Based Security Training

AT-4 Security Training Records

Audit and Accountability (AU) - 11 controls

AU-1 Audit and Accountability Policy and Procedures

AU-2 Audit Events

AU-3 Content of Audit Records

AU-4 Audit Storage Capacity

AU-5 Response to Audit Processing Failures

AU-6 Audit Review, Analysis, and Reporting

AU-8 Time Stamps

AU-9 Protection of Audit Information

AU-10 Non-Repudiation

AU-11 Audit Record Retention

AU-12 Audit Generation

Security Assessment and Authorization (CA) - 9 controls

CA-1 Security Assessment and Authorization Policy and Procedures

CA-2 Security Assessments

CA-3 System Interconnections

CA-5 Plan of Action and Milestones

CA-6 Security Authorization

CA-7 Continuous Monitoring

CA-7(4) Continuous Monitoring | Risk Monitoring

CA-8 Penetration Testing

Implementation:

CA-9 Internal System Connections

Configuration Management (CM) - 11 controls

CM-1 Configuration Management Policy and Procedures

CM-2 Baseline Configuration

CM-3 Configuration Change Control

CM-3(2) Testing, Validation, and Documentation of Changes

CM-4 Security Impact Analysis

CM-5 Access Restrictions for Change

CM-6 Configuration Settings

CM-7 Least Functionality

CM-8 Information System Component Inventory

CM-10 Software Usage Restrictions

CM-11 User-installed Software

Contingency Planning (CP) - 9 controls

CP-1 Contingency Planning Policy and Procedures

CP-2 Contingency Plan

CP-3 Contingency Training

CP-4 Contingency Plan Testing

CP-6 Alternate Storage Site

CP-9 Information System Backup

CP-9(3) Separate Storage for Critical Information

CP-10 Information System Recovery and Reconstitution

CP-11 Alternate Communications Protocols

Identification and Authentication (IA) - 11 controls

IA-1 Identification and Authentication Policy and Procedures

IA-2 Identification and Authentication (Organizational Users)

IA-2(1) Multifactor Authentication to Privileged Accounts

IA-2(2) Multifactor Authentication to Non-Privileged Accounts

IA-4 Identifier Management

IA-5 Authenticator Management

IA-6 Authenticator Feedback

IA-7 Cryptographic Module Authentication

IA-8 Identification and Authentication (Non-Organizational Users)

IA-11 Re-Authentication

IA-12 Identity Proofing

Incident Response (IR) - 9 controls

IR-1 Incident Response Policy and Procedures

IR-2 Incident Response Training

IR-3 Incident Response Testing

IR-4 Incident Handling

IR-5 Incident Monitoring

IR-6 Incident Reporting

IR-7 Incident Response Assistance

IR-8 Incident Response Plan

IR-9 Information Spillage Response

Maintenance (MA) - 4 controls

MA-1 System Maintenance Policy and Procedures

MA-2 Controlled Maintenance

MA-4 Nonlocal Maintenance

MA-5 Maintenance Personnel

Media Protection (MP) - 5 controls

MP-1 Media Protection Policy and Procedures

MP-2 Media Access

MP-3 Media Marking

MP-6 Media Sanitization

MP-7 Media Use

Physical and Environmental Protection (PE) - 11 controls

PE-1 Physical and Environmental Protection Policy and Procedures

PE-2 Physical Access Authorizations

PE-3 Physical Access Control

PE-6 Monitoring Physical Access

PE-8 Visitor Access Records

PE-12 Emergency Lighting

PE-13 Fire Protection

PE-14 Temperature and Humidity Controls

PE-15 Water Damage Protection

PE-16 Delivery and Removal

PE-17 Alternate Work Site

PE-18 Location of System Components

Planning (PL) - 3 controls

PL-1 Security Planning Policy and Procedures

PL-2 System Security Plan

PL-4 Rules of Behavior

Program Management (PM) - 12 controls

PM-1 Information Security Program Plan

PM-2 Senior Information Security Officer

PM-3 Information Security Resources

PM-4 Plan of Action and Milestones Process

PM-5 Information System Inventory

PM-6 Information Security Measures of Performance

PM-7 Enterprise Architecture

PM-9 Risk Management Strategy

PM-10 Authorization Process

PM-14 Testing, Training, Monitoring

PM-15 Security and Privacy Groups and Associations

PM-16 Threat Awareness Program

Personnel Security (PS) - 8 controls

PS-1 Personnel Security Policy and Procedures

PS-2 Position Risk Designation

PS-3 Personnel Screening

PS-4 Personnel Termination

PS-5 Personnel Transfer

PS-6 Access Agreements

PS-7 Third-party Personnel Security

PS-8 Personnel Sanctions

Personally Identifiable Information Processing and Transparency (PT) - 2 controls

PT-1 Policy and Procedures

PT-3 Personally Identifiable Information Processing Purposes

Risk Assessment (RA) - 6 controls

RA-1 Risk Assessment Policy and Procedures

RA-2 Security Categorization

RA-3 Risk Assessment

RA-3(1) Supply Chain Risk Assessment

RA-5 Vulnerability Scanning

RA-7 Risk Response

Implementation:

System and Services Acquisition (SA) - 10 controls

SA-1 System and Services Acquisition Policy and Procedures

SA-2 Allocation of Resources

SA-3 System Development Life Cycle

SA-4 Acquisition Process

SA-5 Information System Documentation

SA-8 Security Engineering Principles

SA-9 External Information System Services

SA-10 Developer Configuration Management

SA-11 Developer Security Testing and Evaluation

SA-22 Unsupported System Components

System and Communications Protection (SC) - 11 controls

SC-1 System and Communications Protection Policy and Procedures

SC-5 Denial of Service Protection

SC-7 Boundary Protection

SC-8 Transmission Confidentiality and Integrity

SC-12 Cryptographic Key Establishment and Management

SC-13 Cryptographic Protection

SC-15 Collaborative Computing Devices

SC-20 Secure Name / Address Resolution Service (Authoritative Source)

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

SC-22 Architecture and Provisioning for Name / Address Resolution Service

SC-39 Process Isolation

System and Information Integrity (SI) - 6 controls

SI-1 System and Information Integrity Policy and Procedures

SI-2 Flaw Remediation

SI-3 Malicious Code Protection

SI-4 Information System Monitoring

SI-5 Security Alerts, Advisories, and Directives

SI-12 Information Handling and Retention

SI-10 Information Input Validation

Supply Chain Risk Management (SR)- 6 controls

SR-1 Policy and Procedures

SR-2 Supply Chain Risk Management Plan

SR-3 Supply Chain Controls and Processes

SR-5 Strategies, Tools, and Methods

SR-8 Notification Agreements

SR-12 Component Disposal

Data Minimization and Retention (DM) - 1 control

DM-1 Minimization of Personally Identifiable Information

Transparency (TR) - 1 control

TR-1 Privacy Notice

Acronyms and Abbreviations

Revision History

Security Controls Standards Catalog

Access Control (AC) – 16 controls

AC-1 Access Control Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (AC-1)

Implementation

TAMU-CC shall:

1. Develop, document, and disseminate to Chief Information Security and Privacy Officer (CISPO):
    a. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Review and update the current:
    a. Access control policy annually; and
    b. Access control procedures annually.
3. Create, distribute, and implement an account management policy which defines the rules for establishing user identity, administering user accounts, and establishing and monitoring user access to information resources
4. Ensure adequate processes are in place to positively establish the identity of (identity-proof) a user and determine the appropriate user role(s) before access is granted.

AC-2 Account Management

Description

Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems.

The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access.

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day of-week, and point-of-origin.

In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Failure to consider these factors could affect information system availability.

Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates.

Conditions for disabling or deactivating accounts include, for example:

i. when shared/group, emergency, or temporary accounts are no longer required; or
ii. when individuals are transferred or terminated. Some types of information system accounts may require specialized training.

Related Controls

- AC-3
- AC-5
- AC-6
- AC-17
- AC-19
- AC-20

- AU-9
- IA-2
- IA-4
- IA-5
- IA-8
- CM-6
- CM-11
- MA-4
- MA-5
- PL-4
- 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.

TAMUS Control (AC-2)

Implementation

TAMU-CC shall:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: An approval process is required prior to granting access authorization for an information resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use (Information Resource-related Rules and TAMU-CC Information Security Controls) and the granting of authorization by the resource owner or their designee;

2. Assigns account managers for information system accounts. Each person is to have a unique logon ID and associated account for accountability purposes. Role accounts (e.g., guest or visitor) are to be used in very limited situations and must provide individual accountability;
3. Establishes conditions for group and role membership. Access authorization controls are to be modified appropriately as an account holder's employment or job responsibilities change;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by Primary Custodian for requests to create information system accounts. Account creation processes are required to ensure only authorized individuals receive access to information resources.
    a. Individuals shall have the ability to access those transactions and functions for which they are authorized;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with the TAMU-CC Security Control Catalog.
    a. Processes are required to disable logon IDs that are associated with individuals who are no longer employed by, or associated with, the University. In the event that the access privilege is to remain active, the department (e.g., owner, department head) shall document that a benefit to the University exists;
    b. All new logon IDs that have not been accessed within a reasonable period of time (as established by risk management decisions) from the date of creation will be disabled

   c. All logon IDs that have not been used/accessed within a period of six months shall be disabled. Exceptions can be made where there is an established unit procedure. These actions shall be reviewed and approved by the unit head. Documentation of exceptions shall be maintained by the information resource owner or designee.
   d. Passwords associated with logon IDs shall comply with all Identification and Authentication security controls.

7. Monitors the use of information system accounts;
8. Information custodians or other designated staff:
   a. Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to TAMU information resources.
   b. Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
   c. Shall periodically review existing accounts for account management compliance.
9. Authorizes access to the information system based on:
   a. A valid access authorization;
   b. Intended system usage; and
   c. Other attributes as required by the organization or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements annually; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

12. Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from one TAMU-CC department to another or from a TAMU-CC department to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing TAMU-CC department.
13. TAMU-CC implements role-based (e.g., students, employees, third parties, guests) access control or adopts a secure Single Sign-on access to cloud and local services (InCommon Federation assurance profile InCommon), where possible.

AC-2(7) Privileged User Accounts

Description:

Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

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: (delay effective date: 08/01/2022)

1. Establish and administer privileged user accounts in accordance with *a role-based access scheme*;
2. Monitor privileged role or attribute assignments;
3. Monitor changes to roles or attributes; and
4. Revoke access when privileged role or attribute assignments are no longer appropriate.
5. Ensure users with privileged (also known as administrative or special access) accounts are aware of the extraordinary responsibilities associated with the use of privileged accounts.

AC-3 Access Enforcement

Description

Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

Related Controls

- AC-2
- AC-5
- AC-6
- AC-17
- AC-18
- AC-19
- AC-20
- AC-22
- AU-9
- CM-6
- CM-11
- MA-4
- MA-5
- PE-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.

TAMUS Control (AC-3)

Implementation

TAMU-CC shall enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

1. Access to University information resources shall be appropriately managed.
2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access. The Primary Custodian of an information resource shall authenticate a user's identity before granting that user access to the information resource.

AC-3(7) Role-based Access Control

Description:

Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3(3) define the scope of the subjects and objects covered by the policy.

Applicability:

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

Implementation: (delay effective date: 08/01/2022)

Implement role-based (e.g., students, employees, third parties, guests) access control or adopt an InCommon Federation assurance profile roles, where possible.

AC-5 Separation of Duties

Description

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example:

i. dividing mission functions and information system support functions among different individuals and/or roles;

ii. conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and

iii. ensuring security personnel administering access control functions do not also administer audit functions.

Related Controls

- AC-3
- AC-6
- PE-3
- PS-2

Applicability

The owner of an information resource, or designee, is responsible for identifying the relevant information technology roles for custodians or users of their information resources.

Separation of duties must be implemented such that operational information resource functions are separated into distinct jobs to prevent a single person from harming a development or operational information resource or the services it provides, whether by an accidental act, omission, or intentional act.

TAMUS Control (AC-5)

Implementation

TAMU-CC shall:

1. Separation of the development, test and operational environments will be implemented, either logically or physically:
    a. Development and operational software must, where possible, run on different computer processors, or in different domains and directories;
    b. Development and testing activities must be separated; and
    c. Compilers, editors, and other system utilities must not be accessible from operational systems when not required.
2. Each individual who uses administrator or special access accounts shall use the account or access privilege most appropriate for the requirements of the work being performed (e.g., user account vs. administrator account).
3. TAMU-CC shall maintain a list(s) of personnel who have administrator or special access accounts for unit information resources. The list(s) shall be reviewed at least annually by the appropriate unit head, information resource owner or their designee.

4. In the course of their normal duties to assure the availability, integrity, utility, authenticity and confidentiality of information resources, information resources custodians with special access privileges may routinely access descriptive data to investigate various events related to the performance or security of those resources. Personnel from the Division of IT may also routinely investigate events related to the performance and the secure operation of the TAMU-CC network. Information resource owners may at times also access user data in maintaining the operational integrity and security of information resources. Information resource custodians shall, however, maintain the confidentiality of user data to the extent practical and not divulge user data except to authorized university officials (such as described in Section 3).
5. In situations requiring special access privileges to conduct investigations, the Chief Information Security and Privacy Officer, shall seek authorization to access the files and email accounts of individuals employed by or attending TAMU-CC, as follows:
    a. Faculty/Staff
        i. For access to accounts involving Faculty & Staff, approval must be obtained from any three (3) of the following:
            1. President
            2. Provost/Vice-President for Academic Affairs
            3. Vice-President for Finance & Administration
            4. Chief Ethics & Compliance Officer
            5. Director, Employee Development & Compliance Services
    b. Students
        i. For access to accounts involving Students, approval must be obtained from any three (3) of the following:
            1. President
            2. Vice-President for Student Affairs
            3. Dean of Students
            4. Associate Dean of Students

        5. Senior Student Conduct Officer

6. Investigations conducted beyond the normal routines outlined in Section 4 and involving user data shall ensure that any user data is revealed only to disinterested third parties as outlined in Section 4 and all the requirements of privacy laws are maintained (e.g., Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, the Texas Public Information Act).
7. In those cases where law enforcement agencies request access in conjunction with an investigation, the request shall be in writing (e.g., subpoena, court order). All such requests shall be reported to the appropriate unit head, director, or their designee upon receipt as well as the Office of General Counsel.
8. Each individual who uses administrator or special access accounts shall use the account or access privilege most appropriate for the requirements of the work being performed (e.g., user account vs. administrator account).
9. The password for a shared administrator or special access account shall change under any one of the following conditions:
    a. an individual knowing the password leaves the Texas A&M department:
    b. job duties change such that the individual no longer performs functions requiring administrator or special access; or
    c. a contractor or vendor with such access leaves or completes their work.
10. In the case where an information resource has only one administrator account, there shall be a password escrow procedure in place such that an appropriate individual other than the person assigned an administrator account can gain access to the account in an emergency situation.
11. When special access accounts are needed for internal or external audit, software development, software installation or other defined need, the need must be:
    a. authorized such as those situations specified in Section 4;
    b. created with a specific expiration date; and
    c. removed when the work is complete.

12. TAMU-CC shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

AC-6 Least Privilege

Description

Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions.

Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege.

Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

Related Controls

- AC-2
- AC-3
- AC-5
- CM-6
- CM-7
- PL-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.

TAMUS Control (AC-6)

Implementation

TAMU-CC shall employ least privilege for routine tasks, and that privileges shall be escalated only as required for a specific action, as follows:

1. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
2. Ensures users with privileged (also known as administrative or special access) accounts are aware of the extraordinary responsibilities associated with the use of privileged accounts.

AC-7 Unsuccessful Login Attempts

Description

This Control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

Related Controls

- AC-2
- AC-14
- IA-5

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.

TAMUS Control (AC-7)

Implementation

1. Enforces a limit of ten (10) consecutive invalid logon attempts by a user during a ten (10) minute time period; and
2. Accounts locked out due to multiple incorrect logon attempts should stay locked out for a minimum of 15 minutes. Accounts for Moderate or High-risk systems should remain locked until reset by an administrator.

AC-8 System Use Notification

Description

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

Applicability

This Control applies to all TAMU-CC information resources.

The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

TAMUS Control (AC-8)

Implementation

System identification/logon banners shall have warning statements that include the following topics:

(a) Unauthorized use is prohibited;

(b) Usage may be subject to security testing and monitoring;

(c) Misuse is subject to criminal prosecution; and

(d) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

The information system shall:

1. Display a TAMU-CC approved banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance and states that:
    a. Users are accessing a U.S. Government information system;
    b. Information system usage may be monitored, recorded, and subject to audit;
    c. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
    d. Use of the information system indicates consent to monitoring and recording;
2. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
    a. Displays TAMU-CC system use information during login, before granting further access;
    b. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    c. Includes a description of the authorized uses of the system.
4. Publish a privacy notice on websites owned by the organization which contains, at a minimum, the content contained on the Texas A&M University System website at https://www.tamus.edu/marcomm/reports/privacy.

AC-11 Session Lock

Description

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.

Related Controls

- AC-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 resource owners and custodians.

TAMUS Control (AC-11)

Implementation

The information system:

1. Custodians shall configure servers such that:
    a. Sessions are locked after 15 minutes of inactivity or upon receiving a request from the session user, and
    b. The session lock remain in effect until the user re-establishes access using established identification and authentication procedures.
2. Custodians shall configure workstations and other endpoint devices such that:
    a. Sessions are locked after 15 minutes of inactivity or upon receiving a request from the session user, except for the following workstation types:
        i. Conference room workstation sessions are locked after 60 minutes of inactivity or upon receiving a request from the session user;

  ii. Classroom workstation sessions are locked after 120 minutes of inactivity or upon receiving a request from the session user;
  iii. Kiosk workstations and special event workstations sessions are exempt from session lockout;
 b. The session lock remain in effect until the user re-establishes access using established identification and authentication procedures.

3. Custodians shall configure session lock screens to completely conceal any information previously visible on the display. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

AC-14 Permitted Actions Without Identification or Authentication

Description

This Control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems.

Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received.

Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use.

This Control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred.

Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none.

Related Controls

- CP-2
- IA-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.

TAMUS Control (AC-14)

Implementation

TAMU-CC Custodians shall:

1. Not permit users to perform any action on an information system without identification or authentication. The sole exception to this is Kiosk workstations; and
2. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

The TAMU-CC identifies, documents, and provides supporting rationale in the security plan for any actions that may be performed on an information system without identification or authentication.

AC-17 Remote Access

Description

Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless.

Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections.

The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code.

Remote access controls apply to information systems other than public web servers or systems designed for public access. This Control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this Control.

Enforcing access restrictions for remote connections is addressed in AC-3.

Related Controls

- AC-2
- AC-3
- AC-18
- AC-19
- AC-20
- CA-3
- CA-7
- CM-8
- IA-2
- IA-8
- MA-4
- PL-4

- SI-4

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.

TAMUS Control (AC-17)

Implementation

TAMU-CC shall:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed by the Information Resource Manager (IRM) approving only those methods for remote access to University information resources or Sensitive Information that encrypt all communications. Examples of such methods are Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), Transport Layer Security (TLS), and Secure Sockets Layer (SSL); and
2. Custodians shall:
    a. Ensure devices and communications are encrypted for University information resources or Sensitive Information.
    b. Affirm their compliance with this policy in the annual risk assessment.
    c. Establish, document, and review usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
    d. All remote access connections (e.g., Virtual Private Network or Remote Desktop) must be authorized prior to allowing such connections.
3. Office of Information Security (OIS) shall:
    a. Review affiliate accounts, which includes remote access used by non-student, non-staff, non-faculty personnel shall be reviewed annually.

4. Networks shall:
    a. Enforce the requirement of multi-factor authentication (MFA) for remote access to TAMU-CC University resources.

AC-18 Wireless Access

Description

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

Related Controls

- AC-2
- AC-3
- AC-17
- AC-19
- CA-3
- CA-7
- CM-8
- IA-2
- IA-8
- PL-4
- SI-4

Applicability

The TAMU-CC Wireless Access Control applies equally to all groups and individuals that utilize wireless connectivity to access TAMU-CC information resources.

This includes students, faculty, and staff members as well as guest account users, vendors, and research partners.

Wireless installation requests should be sent by email message to the Division of IT at ITHelp@tamucc.edu.

TAMUS Control (AC-18)

TAMU-CC shall establish the requirements and security restrictions for installing or providing access to the state organization information resources systems, as follows:

1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access. The network Custodian shall ensure that all University-provided wireless access shall be password protected and that access to that wireless service shall be linked to an individual through authentication mechanisms; and
2. Authorize wireless access to the information system prior to allowing such connections.
3. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting. Some networks should not include organizational or location information in the SSID. Additional equipment configuration recommendations are included in the Wireless Security Guidelines.
4. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information. TAMU-CC shall not transmit confidential information via a wireless connection to, or from a portable computing device unless encryption methods, such as a Virtual Private Network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards, are used to protect the information. All users shall ensure that if they send confidential information over any wireless network, either
    a. the data itself is encrypted,
    b. the link is encrypted (e.g., VPN, HTTPS, Secure FTP), or
    c. both the data and link are encrypted.

5. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organizational IT systems by individuals without the approval of the state organization information resources manager. The network infrastructure Custodian shall routinely scan for unapproved network devices (e.g., rogue wireless access points).

AC-19 Access Control for Mobile Devices

Description

A mobile device is a computing device that:

i. has a small form factor such that it can easily be carried by a single individual;
ii. is designed to operate without a physical connection (e.g., wirelessly transmit or receive information);
iii. possesses local, non-removable or removable data storage; and
iv. includes a self-contained power source.

Mobile devices may also include voice communication capabilities, onboard sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets.

Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device.

The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example:

i. configuration management,
ii. device identification and authentication,

iii. implementation of mandatory protective software (e.g., malicious code detection, firewall),
iv. scanning devices for malicious code,
v. updating virus protection software,
vi. scanning for critical software updates and patches,
vii. conducting primary operating system (and possibly other resident software) integrity checks, and
viii. disabling unnecessary hardware (e.g., wireless, infrared).

Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this Control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process.

There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls.

AC-20 addresses mobile devices that are not organization-controlled.

Related Controls

- AC-3
- AC-7
- AC-18
- AC-20
- CA-9
- CM-2
- IA-2
- MP-2
- PL-4
- SC-7
- SI-3
- SI-4

Applicability

This Control applies to all mobile computing and storage devices that utilize information resources, especially those which process, store, or transmit 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 is all users of TAMU-CC information resources.

TAMUS Control (AC-19)

Implementation

TAMU-CC shall establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for University-controlled mobile devices, whether owned by the TAMU-CC or the employee:

1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for University-controlled mobile devices.; and
2. Authorize the connection of mobile devices to organizational information systems.

AC-20 Use of External Information Systems

Description

External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness.

External information systems include, for example:

(i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants);

(ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports);

(iii) information systems owned or controlled by nonfederal governmental organizations; and

(iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations.

This Control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, executive orders, directives, or policies.

Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments.

This Control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through USAGov).

Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum:

i. types of applications that can be accessed on organizational information systems from external information systems; and
ii. the highest security category of information that can be processed, stored, or transmitted on external information systems.

If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related Controls

- AC-3
- AC-17
- AC-19
- CA-3
- PL-4
- SA-9

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.

TAMUS Control (AC-20)

Implementation

The University establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and

2. Process, store, or transmit organization-controlled information using external information systems.
3. TAMU-CC shall develop policies governing the use of external information systems and resources including the type and classification of data that can be stored outside of the state organization.
4. TAMU-CC shall establish terms and conditions for contracting with external information resources providers.

AC-22 Publicly Accessible Content

Description

In accordance with federal laws, executive orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information).

This Control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication.

The posting of information on non-organization information systems is covered by organizational policy.

Related Controls

- AC-3
- AT-2
- AT-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.

This Control does not apply to faculty or student use of information resources for limited public forums; however, such use should follow TAMU-CC Acceptable Use Policy, Acceptable Use, Section 1.

TAMUS Control (AC-22)

Implementation

TAMU-CC shall:

1. Designate individuals authorized to post information onto a publicly accessible information system. The IRM will designate a Primary Custodian ("webmaster") for all TAMU-CC websites. No website will be launched on the “.tamucc.edu” domain without the approval of the webmaster;
2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Primary custodian (or designee) shall during the annual risk assessment process review the content on the publicly accessible information system for nonpublic information and removes such information, if discovered.
5. Develop policies governing the procedures to post information on publicly accessible information systems.
6. Ensure organizational security controls are applied to official social media use by the member.

Awareness and Training (AT) - 4 controls

AT-1 Awareness and Training Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

This Control applies to all users of TAMU-CC information resources.

TAMUS Control (AT-1)

Implementation

TAMU-CC shall:

1. Chief Information Security and Privacy Officer (CISPO) shall develop, document, and disseminate to TAMU-CC:
    a. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Chief Information Security and Privacy Officer (CISPO) shall review and updates the current:
    a. Security awareness and training policy at least annually; and
    b. Security awareness and training procedures at least annually.

3. Chief Information Security and Privacy Officer (CISPO) shall establish the requirements to ensure each user of information resources receives adequate training on computer security issues.

AT-2 Security Awareness Training

Description

Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access.

The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security.

Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Related Controls

- AT-3
- AT-4
- PL-4

Applicability

This Control applies to all TAMU-CC personnel who use University information resources.

TAMUS Control (AT-2)

Implementation

TAMU-CC through the Chief Information Security and Privacy Officer (CISPO) shall provide basic security awareness training to information system users including employees, contingent workers, and affiliates. Such workforce members (includes, but is not limited to managers, senior executives, and contractors) (TAMU-CC Procedure 33.05.02.C0.01, Required Training for Employees and Affiliates [TAMU-CC 33.05.02.C0.01]). Basic security awareness training shall include:

1. As part of initial training for new users, TAMU-CC shall conduct new employee orientation to introduce information security awareness and inform new employees of information security policies and procedures;
2. When required by information systems, TAMU System, state, federal, and/or regulatory requirements change;
3. Annually shall provide an ongoing information security awareness education program for all users; and
4. Refresher trainings following security or privacy events when deemed necessary by the Chief Information Security and Privacy Officer.

AT-3 Role-Based Security Training

Description

Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide

i. enterprise architects,
ii. information system developers,
iii. software developers,
iv. acquisition/procurement officials,
v. information system managers,
vi. system/network administrators,
vii. personnel conducting configuration management and auditing activities,
viii. personnel performing independent verification and validation activities,
ix. security control assessors, and
x. other personnel having access to system-level software

adequate security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined.

Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

Role-based security training also applies to contractors providing services to federal agencies.

Related Controls

- AT-2
- AT-4
- PL-4
- PS-7
- SA-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.

TAMUS Control (AT-3)

Implementation

TAMU-CC shall provide role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. Annually thereafter.

AT-4 Security Training Records

Description

Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Related Controls

- AT-2
- AT-3
- PM-14

Applicability

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

TAMUS Control (AT-4)

Implementation

TAMU-CC shall:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records according to the TAMU-CC records retention schedule as stated in State of Texas SLR 105 Rev. 2017-07.
3. TAMU-CC shall maintain information security awareness and training records via TrainTraq.

Audit and Accountability (AU) - 11 controls

AU-1 Audit and Accountability Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (AU-1)

Implementation

TAMU-CC Chief Information Security and Privacy Officer (CISPO) shall:

1. Develop, documents, and disseminates to TAMU-CC employees, contingent workers, and affiliates. Such workforce members include, but are not limited to, managers, senior executives, and contractors:

  a. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  b. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

2. Reviews and updates the current:
   a. Audit and accountability policy annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change and
   b. Audit and accountability procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.
3. TAMU-CC develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

AU-2 Audit Events

Description

An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs.

Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage.

In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this Control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, executive orders, directives, policies, regulations, and standards.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.

Related Controls

- AC-6
- AC-17
- AU-3
- AU-12
- MA-4
- MP-2
- SI-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.

TAMUS Control (AU-2)

Implementation

TAMU-CC Chief Information Security and Privacy Officer (CISPO) shall:

1. Determines that the information system is capable of performing an audit. Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited annually, or when the situation of auditing requires, within the information system:
    a. All logins, successful or unsuccessful;
    b. All logouts;
    c. Changes to automated security rules (e.g., firewall settings, anti-virus settings, intrusion detection parameters);
    d. Changes to audit and logging settings;
    e. Privilege escalations (e.g., sudo);
    f. Establishing system accounts;
    g. Configuring access authorizations (i.e., permissions; privileges).
5. Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware, and software and for all changes to automated security or access rules.

6. Based on the risk assessment, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.

AU-3 Content of Audit Records

Description

Audit record content that may be necessary to satisfy the requirement of this Control, includes, for example:

i. time stamps,
ii. source and destination addresses,
iii. user/process identifiers,
iv. event descriptions,
v. success/fail indications,
vi. filenames involved, and
vii. access control or flow control rules invoked.

Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).

To learn more, see NIST Special Publication 800-92.

Related Controls

- AU-2
- AU-8
- AU-12

Applicability

This Control applies to all TAMU-CC information resources containing controlled 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.

TAMUS Control (AU-3)

Implementation

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit record content includes, for most audit records:

1. date and time of the event;
2. the component of the information system (e.g., software component, hardware component) where the event occurred;
3. type of event;
4. user/subject identity; and
5. the outcome (success or failure) of the event.

NIST Special Publication 800-92 provides guidance on computer security log management.

AU-4 Audit Storage Capacity

Description

Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Related Controls

- AU-2
- AU-5
- AU-6
- AU-11
- SI-4

Applicability

This Control applies to all TAMU-CC University information resources containing essential, controlled, 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.

TAMUS Control (AU-4)

Implementation

TAMU-CC shall allocate audit record storage capacity to ensure there is sufficient storage capacity to retain at least one years' worth of log data. TAMU-CC shall allocate sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

AU-5 Response to Audit Processing Failures

Description

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors).

This Control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Related Controls

- AU-4
- SI-12

Applicability

This Control applies to all TAMU-CC University information resources containing controlled 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.

TAMUS Control (AU-5)

Implementation

The information system:

1. Alerts appropriate organizational officials in the event of an audit processing failure; and
2. Takes the following additional actions may including, but not limited to:
    a. alert the Office of Information Security (OIS) of logging failure
    b. troubleshoot root cause of failure
    c. log failure of event
    d. shut down information system
    e. overwrite oldest audit records if older that retention stated in AU-4 and AU-11
    f. stop generating audit records with approval of Office of Information Security (OIS)

AU-6 Audit Review, Analysis, and Reporting

Description

Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of

i. account usage,
ii. remote access,
iii. wireless connectivity,
iv. mobile device connection,
v. configuration settings,

vi. system component inventory,

vii. use of maintenance tools and nonlocal maintenance,

viii. physical access,

ix. temperature and humidity,

x. equipment delivery and removal,

xi. communications at the information system boundaries,

xii. use of mobile code, and

xiii. use of VoIP.

Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department.

If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.

Related Controls

- AC-2
- AC-3
- AC-6
- AC-17
- AT-3
- CA-7
- CM-10
- CM-11
- IA-5
- IR-5
- IR-6
- MA-4
- PE-3
- PE-6

- PE-14
- PE-16
- RA-5
- SC-7
- SI-3
- SI-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.

TAMUS Control (AU-6)

Implementation

1. TAMU-CC Primary Custodian regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to the Chief Information Security and Privacy Officer (CISPO), and takes necessary actions, including:
   a. The Primary Custodian of Critical 1 critical server or system shall ensure that the logs from that server or system are reviewed daily.
   b. The Primary Custodian of Critical 2 critical server or system shall ensure that the logs from that server or system are reviewed daily.
   c. The Primary Custodian of Critical 3 critical server or system shall ensure that the logs from that server or system are reviewed weekly.
   d. The Primary Custodian of a server or system that is neither Critical 1, Critical 2 nor Critical 3 critical shall ensure that the logs from that server or system are reviewed monthly. Reports findings to the Chief Information Security and Privacy Officer (CISPO) and Primary Business Owner.

AU-8 Time Stamps

Description

Time stamps generated by the information system include date and time.

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.

Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components.

Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls

- AU-3
- AU-12

Applicability

This Control applies to all TAMU-CC University information resources containing 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.

TAMUS Control (AU-8)

Implementation

The information system:

1. Whenever technically possible, information systems should provide time stamps for use in audit record generation;
2. The IRM shall designate a Primary Custodian of the Network Time Service;

3. The Primary Custodian of the Network Time Service shall define one or more permitted authoritative time sources (PATS); and
4. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets:
    a. the system connects to a PATS at least once every 1024 seconds;
    b. if the system's time and the PAT's time differ by more than 60 seconds, the system's time is updated to match the PAT's time.

AU-9 Protection of Audit Information

Description

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

This Control focuses on technical protection of audit information.

Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.

Related Controls

- AC-3
- AC-6
- MP-2
- PE-2
- PE-3
- PE-6

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.

TAMUS Control (AU-9)

Implementation

The information system protects audit information and audit tools from unauthorized access, modification, and/or deletion.

AU-10 Non-Repudiation

Description:

Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC16, SC-17, SC-23.

Applicability:

This Control applies to all TAMU-CC University information resources containing 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: (delay effective date: 07/20/2023)

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed any change, addition, or deletion.

AU-11 Audit Record Retention

Description

Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions.

Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action.

The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.

Related Controls

- AU-4
- AU-5
- AU-9
- MP-6

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.

TAMUS Control (AU-11)

Implementation

The organization retains audit records for at least the last 365 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-12 Audit Generation

Description

Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records.

Related Controls

- AC-3
- AU-2
- AU-3
- AU-6

Applicability

This Control applies to all TAMU-CC University information resources storing or accessing restricted, controlled, or confidential information.

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

TAMUS Control (AU-12)

Implementation

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 (1) utilizing the designated TAMU-CC SIEM;
2. Allows Office of Information Security (OIS) to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2(4) with the content defined in AU-3.

Security Assessment and Authorization (CA) - 9 controls

CA-1 Security Assessment and Authorization Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (CA-1)

Implementation

TAMU-CC Chief Information Security and Privacy Officer (CISPO) shall:

1. Develop, document, and disseminate:

    a. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
    a. Security assessment and authorization annually; and
    b. Security assessment and authorization procedures annually.
3. TAMU-CC shall establish a security assessment procedure.

CA-2 Security Assessments

Description

Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of:

- i initial and ongoing security authorizations;
- ii FISMA annual assessments;
- iii continuous monitoring; and
- iv system development life cycle activities.

Security assessments:

- i. ensure that information security is built into organizational information systems;
- ii. identify weaknesses and deficiencies early in the development process;
- iii. provide essential information needed to make risk-based decisions as part of security authorization processes; and
- iv. ensure compliance to vulnerability mitigation procedures.

Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans.

Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources:

i. initial or ongoing information system authorizations;
ii. continuous monitoring; or
iii. system development life cycle activities.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed.

Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies.

Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures.

External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this Control.

Related Controls

- CA-5
- CA-6
- CA-7
- RA-5
- SI-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.

TAMUS Control (CA-2)

Implementation

TAMU-CC Chief Information Security and Privacy Officer (CISPO) shall:

1. Develops a security assessment plan that describes the scope of the assessment including:
    a. Security controls and control enhancements under assessment;
    b. Assessment procedures to be used to determine security control effectiveness; and
    c. Assessment environment, assessment team, and assessment roles and responsibilities;

2. Assesses the security controls in the information system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to the University Chief Information Officer (CIO) and University President/CEO.
5. A review of the TAMU-CC information security program for compliance with these standards will be performed at least annually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the TAMU-CC President or his or her designated representative(s).

CA-3 System Interconnections

Description

This Control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing.

Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations.

Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems.

Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations.

Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.

Related Controls

- AC-3
- AC-20
- AU-2
- AU-12
- CA-7
- SA-9
- SC-7
- SI-4

Applicability

The intended audience includes information resource owners and custodians.

This Control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing.

TAMUS Control (CA-3)

Implementation

TAMU-CC shall:

1. Authorize connections from information systems to other information systems through the use of Interconnection Security Agreements. The organization authorizes all connections from internal/organization information system to other information systems outside of organization through the use of system connection agreements and monitors/controls the system connections on an ongoing basis;
2. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. Primary Custodians shall document in Information Resource Inventory System (IRIS) any connection between their systems and other information systems, either inside or outside of TAMU-CC; and
3. Reviews and updates Interconnection Security Agreements annually.

CA-5 Plan of Action and Milestones

Description

Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.

Related Controls

- CA-2
- CA-7
- CM-4
- PM-4

Applicability

The intended audience includes information resource owners and custodians.

TAMUS Control (CA-5)

Implementation

TAMU-CC shall:

1. Develop and update, a plan of action and milestones for the information system that documents the TAMU-CC's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-6 Security Authorization

Description

Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of agreed-upon security controls.

Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks.

OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

Related Controls

- CA-2

- CA-7

Applicability

The intended audience includes information resource owners and custodians.

TAMUS Control (CA-6)

Implementation

TAMU-CC shall:

1. Authorize the information system for processing before operations and when there is a significant change to the system;
2. Ensure that the Primary Custodian authorizes the information system for processing before commencing operations; and
3. Updates the security authorization annually.

CA-7 Continuous Monitoring

Description

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions.

The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies.

Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely.

Continuous monitoring activities are scaled in accordance with the security categories of information systems.

Related Controls

- CA-2
- CA-5
- CA-6
- CM-3
- CM-4
- PM-6
- RA-5
- SI-2
- SI-4

Applicability

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

TAMUS Control (CA-7)

Implementation

TAMU-CC develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. TAMU-CC monitors the security controls in the information system on an ongoing basis;
2. Establishment of at least monthly monitoring and annually for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the TAMU-CC continuous monitoring strategy;

4. Ongoing security status monitoring of organization-defined metrics in accordance with the TAMU-CC continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to Chief Information Office and University President/CEO annually.

CA-7(4) Continuous Monitoring | Risk Monitoring

Description:

Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Applicability:

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

Implementation: (delay effective date: 07/20/2023)

TAMU- CC shall ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

1. Effectiveness monitoring;
2. Compliance monitoring; and
3. Change monitoring.

CA-8 Penetration Testing

Description:

Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

Applicability:

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

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall conduct penetration testing annually and additionally following significant infrastructure changes on external facing information systems.

CA-9 Internal System Connections

Description

This Control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers.

Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

Related Controls

- AC-3
- AC-18
- AC-19
- AU-2
- AU-12
- CA-7
- CM-2
- SC-7
- SI-4

Applicability

The intended audience includes information resource owners and custodians.

This Control applies to dedicated internal connections between information systems (i.e., intra-system connections) and does not apply to transitory, user-controlled connections such as email and website browsing.

TAMUS Control (CA-9)

Implementation

TAMU-CC shall:

1. TAMU-CC has a procedure for authorizing internal information resource connections to:
    a. Attach a device to a TAMU-CC network only if that device complies with all applicable policy (see especially CM-06);
    b. Attach only TAMU-CC-owned or -managed devices to a privileged TAMU-CC network;
    c. Attach non-TAMU-CC-owned or -managed devices only to an unprivileged TAMU-CC network;
    d. Attach a device to a privileged TAMU-CC network only if the device is recorded in the Inventory;
    e. Make a device directly accessible from the Internet (e.g., by NAT'ing a publicly routable IP address to the server's private address), only if:
        i. The devices are in a DMZ designated for Internet-accessible devices, and
        ii. OIS approves.
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Configuration Management (CM) - 11 controls

CM-1 Configuration Management Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (CM-1)

Implementation

TAMU-CC Chief Information Security and Privacy Officer (CISPO) shall:

1. Develop document and disseminate to custodians:
    a. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Review and update the current:
    a. Configuration management policy annually; and
    b. Configuration management procedures annually.
3. TAMU-CC shall control modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during, and after system implementation.

CM-2 Baseline Configuration

Description

This Control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems.

Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time.

Baseline configurations of information systems reflect the current enterprise architecture.

Related Controls

- CM-3
- CM-6
- CM-8
- SA-10
- PM-5
- PM-7

Applicability

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

TAMUS Control (CM-2)

Implementation

TAMU-CC shall

1. Develop, document, and maintain under configuration control, a current baseline configuration of the information system.
2. Ensure all servers on System-owned or -managed networks conform to a baseline security configuration and are security-hardened based on risk. The Primary Custodian of an information resource shall develop, document, and maintain a current baseline configuration of the information resource.
3. Detail the listing of supported operating systems for servers and workstations. Unsupported operating systems shall have an exception on file with a targeted remediation date and mitigating controls sufficient to reduce the risk to an acceptable level.

CM-3 Configuration Change Control

Description

Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications.

Configuration change control includes

i. changes to baseline configurations for components and configuration items of information systems,
ii. changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices),
iii. unscheduled/unauthorized changes, and
iv. changes to remediate vulnerabilities.

Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems.

For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards.

Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

Related Controls

- CA-7
- CM-2
- CM-4
- CM-6
- SA-10
- SI-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 is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

TAMUS Control (CM-3)

Implementation

TAMU-CC incorporates change management processes to ensure secure, reliable, and stable operations to which all offices that support information systems adhere. The change management process incorporates guidelines that address:

1. Determines the types of changes to the information system that are configuration-controlled, formally identifying, classifying, prioritizing, and requesting changes;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses, formally identifying, classifying, prioritizing, and requesting changes;

3. Documents configuration change decisions associated with the information system, identifying and deploying emergency changes;
4. Implements approved configuration-controlled changes to the information system, authorizing changes and exceptions;
5. Retains records of configuration-controlled changes to the information system for at least 365 days, testing changes;
6. Audits and reviews activities associated with configuration-controlled changes to the information system, implementing changes and planning for back-outs, and
7. Coordinates and provides oversight for configuration change control activities through University Technology Council (UTC) and weekly Change Advisory Board (CAB) that convenes, documenting and tracking changes.

CM-3(2) Testing, Validation, and Documentation of Changes

Description:

Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6 . Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures, system security and privacy policies and procedures, and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be taken offline, or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Applicability:

The intended audience is information resource owners and custodians of University information resources that store or process mission critical and/or confidential information.

Implementation: (delay effective date: 08/01/2022)

Test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-4 Security Impact Analysis

Description

Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications.

Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required.

Security impact analyses are scaled in accordance with the security categories of the information systems.

Related Controls

- CA-2
- CA-7
- CM-3
- SA-4
- SA-5

- SA-10
- SI-2

Applicability

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

TAMUS Control (CM-4)

Implementation

TAMU-CC analyzes changes to the information system to determine potential security impacts prior to change implementation.

1. All security-related information resources changes shall be approved by the information owner through a change control process.
    a. All change requests must include a description of the security impact of the change.
    b. The Change Management team shall consider the security impact of a change request during the review process.
2. Approval shall occur prior to implementation by TAMU-CC or independent contractors.

CM-5 Access Restrictions for Change

Description:

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-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: (delay effective date: 07/20/2023)

TAMU-CC defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

CM-6 Configuration Settings

Description

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system.

Information technology products for which security-related configuration settings can be defined include, for example:

i. mainframe computers,
ii. servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name),
iii. workstations,
iv. input/output devices (e.g., scanners, copiers, and printers),
v. network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors),
vi. operating systems,
vii. middleware, and
viii. applications.

Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example:

i. registry settings;
ii. account, file, and directory permission settings; and
iii. settings for functions, ports, protocols, services, and remote connections.

Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements.

Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7.

The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings.

OMB establishes federal policy on configuration requirements for federal information systems.

Related Controls

- AC-19
- CM-2

- CM-3
- CM-7
- SI-4

Applicability

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

TAMUS Control (CM-6)

Implementation

TAMU-CC shall:

1. Establish and document configuration settings for information technology products employed within the information system using security configuration procedure that reflect the most restrictive mode consistent with operational requirements, establishes mandatory configuration settings for information technology products employed within the information system. TAMU-CC adopts baseline security configuration checklists that meet or exceed published industry best practice sources (e.g., Center for Internet Security Benchmarks [CIS Benchmarks], NIST National Checklist Program [NCP]) when available, or locally develops security configuration checklists otherwise, for all System-owned or -managed major and mission-critical information systems, and systems processing confidential information;
2. Implement the configuration settings, configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;
3. Identify, document, and approve any deviations from established configuration settings for information system components based on security configuration procedure, documents the configuration settings; and

4. Monitor and control change to the configuration settings in accordance with organizational policies and procedures. Enforces the configuration settings in all components of the information system.

CM-7 Least Functionality

Description

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components but doing so increases risk over limiting the services provided by any one component.

Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing).

Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.

Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Related Controls

- AC-6
- CM-2
- RA-5

- SA-5
- SC-7

Applicability

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

TAMUS Control (CM-7)

Implementation

TAMU-CC shall:

1. Configures the information system to provide only essential capabilities. Primary Custodians shall configure information resources according to the principles of least functionality; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services:
   a. FTP (Port 21)
   b. Telnet (Port 23)
   c. POP (Port 110)
   d. TFTP (Port 69)
   e. SMTP (Port 25)
   f. DNS (Port 53)
   g. NTP (Port 123)
   h. MS RPC – TCP & UDP (Port 135)
   i. NetBIOS/IP – TCP & UDP (Ports 137-139)
   j. SMB/IP – TCP (Port 445)
   k. Trivial File Transfer Protocol (TFTP) – UDP (Port 69)
   l. Syslog – UDP (Port 514)
   m. Simple Network Management Protocol (SNMP) – UDP (Ports 161-162)
   n. Internet Relay Chat (IRC) – TCP (Ports 6660-6669)

o. Protocols that utilize nonsecure methods (e.g., those that utilize plaintext authentication)

CM-8 Information System Component Inventory

Description

Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner).

Information deemed necessary for effective accountability of information system components includes, for example:

i. hardware inventory specifications,
ii. software license information,
iii. software version numbers,
iv. component owners, and
v. for networked components or devices, machine names and network addresses.

Inventory specifications include, for example:

i. manufacturer,
ii. device type,
iii. model,
iv. serial number, and
v. physical location.

Related Controls

- CM-2
- CM-6
- PM-5

Applicability

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

TAMUS Control (CM-8)

Implementation

TAMU-CC shall:

1. Develop, document, and maintain a current inventory of the components of the information system and relevant ownership information that:
    a. Accurately reflects the current information system;
    b. Includes all components within the authorization boundary of the information system;
    c. Is at the level of granularity deemed necessary for tracking and reporting; and
    d. Includes information deemed necessary to achieve effective information system component accountability; and
2. Reviews and updates the information system component inventory annually.

CM-10 Software Usage Restrictions

Description

Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.

Related Controls

- AC-17
- CM-8
- SC-7

Applicability

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

TAMUS Control (CM-10)

Implementation

TAMU-CC shall ensure software installed on System-owned or -managed information systems is used in accordance with the applicable software license(s) and understands unauthorized or unlicensed use of software is regarded as a serious matter subject to disciplinary action:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws. See TAMU-CC Acceptable Use Policy for a list of prohibited software. The Primary Custodian of a computer shall:
    a. Install a software application on a computer only 1) with the approval of the Primary Custodian of the software application and 2) if such installation is in accordance with all applicable law and policy (including the TAMU-CC Acceptable Use Policy).
    b. Remove from the computer any software application that is in violation of law and policy (including the TAMU-CC Acceptable Use Policy).
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-11 User-installed Software

Description

If provided the necessary privileges, users have the ability to install software in organizational information systems.

To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation.

Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores" Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious.

The policies organizations select governing user-installed software may be organization developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

Related Controls

- AC-3
- CM-2
- CM-3
- CM-6
- CM-7
- PL-4

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.

The intended audience is users of University information resources.

TAMUS Control (CM-11)

Implementation

TAMU-CC shall:

1. All software installed on University-owned or operated computer systems used by faculty members, staff members, agents, or students in the conduct of University business must be appropriately licensed (Texas A&M System Regulation 29.01.02, Use of Licensed Software [TAMUS 29.01.02]).
    a. For software having a licensing agreement, persons installing or authorizing the installation of software should be familiar with the terms of the

agreement. Where feasible, the licensing agreement should be maintained in the department that operates the system on which the software is installed or through a license management agreement with a third party.;

  b. In cases where this is not feasible, individuals or organizations should maintain sufficient documentation (e.g., End User License Agreements, purchase receipts) to validate that the software is appropriately licensed.

2. Enforces software installation policies through endpoint central management tools; and
3. Monitors policy compliance at least annually.
4. See the TAMU-CC document Acceptable Use Policy for a list of prohibited software.

Contingency Planning (CP) - 9 controls

CP-1 Contingency Planning Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (CP-1)

Implementation

TAMU-CC Chief Information Security and Privacy Officer, Owners, and Custodians shall:

1. Develop, document, and disseminate to TAMU-CC:
    a. Chief Information Security and Privacy Officer is responsible for contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Owners, and Custodians are responsible for procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls;
    c. develops information resources contingency planning policy and procedures that align with the TAMU-CC emergency management plan as required by Texas A&M System Regulation 34.07.01, Emergency Management [TAMUS 34.07.01]; and
2. TAMU-CC shall maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimized, and the University will be able either to maintain or quickly resume mission-critical functions; and
3. Reviews and updates the current:
    a. Contingency planning policy annually;
    b. Contingency planning procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

CP-2 Contingency Plan

Description

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised.

The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency.

Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, executive orders, directives, policies, standards, regulations, and guidelines.

In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems.

Actions addressed in contingency plans include, for example:

i. orderly/graceful degradation,
ii. information system shutdown,
iii. fallback to a manual mode,
iv. alternate information flows, and
v. operating in modes reserved for when systems are under attack.

By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

Related Controls

- AC-14
- CP-6
- CP-9
- CP-10
- IR-4
- IR-8
- MP-2

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.

TAMUS Control (CP-2)

Implementation

TAMU-CC shall:

1. Develop a contingency plan for the information system. The plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include, but are not limited to:

a. Identifies essential missions and business functions and associated contingency requirements. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:
    i. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:
        1. Internal and external points of contact for personnel that provide or receive data or support interconnected systems.
        2. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

b. Provides recovery objectives, restoration priorities, and metrics. Disruption impacts and allowable outage times to include:
    i. Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function. ii. Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.

c. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:
    i. Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms. ii. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

d. Addresses contingency roles, responsibilities, assigned individuals with contact information;

    e. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
    f. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    g. Is reviewed and approved by Information Resource Manager (IRM);

2. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.
3. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.
4. Disaster Recovery Plan—TAMU-CC shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:
    a. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;
    b. Identify recovery resources and a source for each;
    c. Contain step-by-step implementation instructions;
    d. Include provisions for annual testing.
5. Coordinates contingency planning activities with incident handling activities;
6. Reviews the contingency plan for the information system annually;
7. Updates the contingency plan to address changes to the University, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
8. Communicates contingency plan changes to Owners and Custodians; and
9. Protects the contingency plan from unauthorized disclosure and modification.

CP-3 Contingency Training

Description

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training.

For example:

i. regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected;

ii. system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and

iii. managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities.

Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

Related Controls

- AT-2
- AT-3
- CP-2
- IR-2

Applicability

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

TAMUS Control (CP-3)

Implementation

TAMU-CC provides contingency training to information system users consistent with assigned roles and responsibilities. TAMU-CC shall train personnel in their contingency roles and responsibilities with respect to the information system and provides periodic refresher training as follows:

1. Within 90 days of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. Annually thereafter.

CP-4 Contingency Plan Testing

Description

Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations.

Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls

- CP-2
- CP-3

Applicability

This Control applies to all mission critical information resources, Essential IT Services, and additional resources as noted.

The information resource owner or designee is responsible for ensuring the recovery and reconstitution procedures are tested.

Based on risk management considerations, the university’s Chief Information Security and 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.

TAMUS Control (CP-4)

Implementation

TAMU-CC shall:

1. Test the contingency plan for the information system annually using tabletop exercise to determine the effectiveness of the plan and the organizational readiness to execute the plan;
    a. Reviews the contingency plan test results; and
    b. Initiates corrective actions, if needed.
2. Test the contingency plan at least every three years with a full interruption of mission-critical, on-premises services, and
3. Include information resources contingency plan testing in the member's emergency management plan testing and exercises.

CP-6 Alternate Storage Site

Description

Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available.

Items covered by alternate storage site agreements include, for example:

i. environmental conditions at alternate sites,
ii. access rules,
iii. physical and environmental protection requirements, and
iv. coordination of delivery/retrieval of backup media.

Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

Related Controls

- CP-2

- CP-9
- CP-10

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.

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.

TAMUS Control (CP-6)

Implementation

TAMU-CC shall:

1. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information;
2. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site; and
3. Ensure mission-critical information shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized TAMU-CC representatives.

CP-9 Information System Backup

Description

System-level information includes, for example, system-state information, operating system and application software, and licenses.

User-level information includes any information other than system level information.

Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes.

Protection of system backup information while in transit is beyond the scope of this Control.

Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

Related Controls

- CP-2
- CP-6
- SC-13

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.

TAMUS Control (CP-9)

Implementation

TAMU-CC conducts backups of system-level information (including system state information) and critical user-level information contained in the information system and protects backup information at the storage location, as follows:

1. Conducts backups of user-level information contained in the information system network storage according to the SLA agreed upon with the data owner;
2. Conducts backups of system-level information contained in the information system as defined by the business impact analysis;

3. Conducts backups of information system documentation including security-related documentation consistent with the requirements of the business impact analysis and
4. Protects the confidentiality, integrity, and availability of backup information at storage locations.
5. TAMU-CC stores backup copies of information systems that process and/or store sensitive or mission-critical information offline or in a separate facility that is not collocated with the operational system.

CP-9(3) Separate Storage for Critical Information

Description:

Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers.

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: (delay effective date: 07/20/2023)

Protect information systems that process and/or store sensitive or high-impact information with a backup strategy which uses immutable backup storage and/or an out-of-band backup process that prevents direct access to backup storage from the organization’s production networks.

CP-10 Information System Recovery and Reconstitution

Description

Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states.

Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements.

Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes:

i. assessments of fully restored information system capabilities,
ii. reestablishment of continuous monitoring activities,
iii. potential information system reauthorizations, and
iv. activities to prepare the systems against future disruptions, compromises, or failures.

Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.

Related Controls

- CA-2
- CA-6
- CA-7
- CP-2
- CP-6
- CP-9

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.

TAMUS Control (CP-10)

Implementation

TAMU-CC shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. TAMU-CC employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

CP-11 Alternate Communications Protocols

Description:

Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

Applicability:

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall provide the capability to employ alternative communications protocols in support of maintaining continuity of operations.

Identification and Authentication (IA) - 11 controls

IA-1 Identification and Authentication Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

This Control applies to all TAMU-CC information resources.

The intended audience for this Control includes all owners, managers, system administrators, and university users of information resources.

TAMUS Control (IA-1)

Implementation

TAMU-CC shall establish policies for verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an information system:

1. Develop, document, and disseminate to Owners and Custodians:
    a. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Review and update the current:
    a. Identification and authentication policy annually; and
    b. Identification and authentication procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

IA-2 Identification and Authentication (Organizational Users)

Description

Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This Control applies to all accesses other than:

i. accesses that are explicitly identified and documented in AC-14; and
ii. accesses that occur through authorized use of group authenticators without individual authentication.

Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof.

Access to organizational information systems is defined as either local access or network access.

- Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks.
- Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses).
- Remote access is a type of network access that involves communication through external networks (e.g., the Internet).

Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this Control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans.

Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as:

i. something you know (e.g., password, personal identification number [PIN]);
ii. something you have (e.g., cryptographic identification device, token); or
iii. something you are (e.g., biometric).

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card.

In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security.

Identification and authentication requirements for other than organizational users are described in IA-8.

Related Controls

- AC-2
- AC-3
- AC-14
- AC-17
- AC-18
- 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.

TAMUS Control (IA-2)

Implementation

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access. Multi-factor Authentication (MFA) will be required when connecting externally.

IA-2(1) Multifactor Authentication to Privileged Accounts

Description:

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Applicability:

This Control applies to all Texas A&M information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall implement multifactor authentication for access to privileged accounts.

IA-2(2) Multifactor Authentication to Non-Privileged Accounts

Description:

Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Applicability:

This Control applies to all Texas A&M information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation: (delay effective date: 07/20/2023)

TAMUCC shall implement multifactor authentication for access to non-privileged accounts.

IA-4 Identifier Management

Description

Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts).

Typically, individual identifiers are the usernames of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4.

This Control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems).

Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Related Controls

- AC-2
- IA-2
- 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.

TAMUS Control (IA-4)

Implementation

TAMU-CC manages information system identifiers by:

1. Receiving authorization from Owners and Custodians to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers;
5. Disabling the identifier after ninety (90) days of inactivity for all accounts except student accounts. Student accounts shall be disabled three hundred sixty-five (365) days after the final day of the last enrolled term; and
6. A user’s access authorization shall be appropriately modified or removed when the user’s employment or job responsibilities within the state organization change.

IA-5 Authenticator Management

Description

Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length).

In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3 and AC-6 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges).

Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example:

i. minimum password length,
ii. password composition,
iii. validation time window for time synchronous one-time tokens, and
iv. number of allowed rejections during the verification stage of biometric authentication.

Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately.

Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

Related Controls

- AC-2
- AC-3
- AC-6
- CM-6
- IA-2
- IA-4
- IA-8
- PL-4
- PS-5
- PS-6
- SC-12
- SC-13

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).

TAMUS Control (IA-5)

Implementation

TAMU-CC manages information system authenticators by:

1. Defining initial authenticator content. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;

3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators every one hundred eighty (180) days;
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts' changes.

Requirements for password complexity based on type of user:

1. Ensure that passwords comply with the following:
    a. Individual interactive account (student, faculty, staff, and affiliate)
        i. Generation: user-chosen or randomly generated by algorithm
        ii. Expiration: 180
        iii. Minimum Length: 8 characters
        iv. Required Complexity. At least three of the following five:
            1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
            2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
            3. Base 10 digits (0 through 9)
            4. Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

v. History: 10 passwords

vi. Min Age: 1 day

b. Administrative Interactive account (.admin, _admin or admin for systems that require a local administrative account)

i. Generation: user-chosen or randomly generated by algorithm

ii. Expiration: 180

iii. Minimum Length: 12 characters

iv. Required Complexity. At least three of the following five:

1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
3. Base 10 digits (0 through 9)
4. Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

v. History: 10 passwords

vi. Min Age: 1 day

c. Service Accounts

i. Generation: Randomly generated by algorithm

ii. Expiration: Never

iii. Minimum Length: 24 chars

iv. Required Complexity. At least three of the following five:

1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)

        2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
        3. Base 10 digits (0 through 9)
        4. Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
        5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

    v. History: 10

    vi. Min Age: 1 day

2. Other precautions should be taken where feasible and relevant:
    a. Limit login to specific source IP address(es);
    b. Turn off interactive login.

IA-6 Authenticator Feedback

Description

The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms.

For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2- to 4-inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly.

Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

Applicability

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (IA-6)

Implementation

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Measures to protect authentication information must be implemented, including, but not limited to:

1. Passwords are masked upon key entry; and
2. Failed login feedback does not indicate which part of the username/password combination was incorrect.

IA-7 Cryptographic Module Authentication

Description

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related Controls

- SC-12
- SC-13

Applicability

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (IA-7)

Implementation

The information system must implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-8 Identification and Authentication (Non-Organizational Users)

Description

Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14.

In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems).

Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk.

IA-2 addresses identification and authentication requirements for access to information systems by organizational users.

Related Controls

- AC-2
- AC-14
- AC-17
- AC-18
- IA-2
- IA-4
- IA-5

- MA-4
- RA-3
- 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.

TAMUS Control (IA-8)

Implementation

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Non-organizational users must be formally authorized to access a given information resource by the account sponsor.

IA-11 Re-Authentication

Description:

In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators, or credentials change, when security categories of syste ms change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Applicability:

This Control applies to all Texas A&M-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation: (delay effective date: 08/01/2022)

Limit the lifetime of browser cookies used for binding authenticated sessions to organization-owned or -managed information systems to no more than five (5) days.

IA-12 Identity Proofing

Description:

Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include

Applicability:

The intended audience for this Control includes all owners and custodians of information resources.

Implementation: (delay effective date: 07/20/2023)

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
b. Resolve user identities to a unique individual; and
c. Collect, validate, and verify identity evidence.

Incident Response (IR) - 9 controls

IR-1 Incident Response Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

This Control applies to all unit heads, information resource owners or custodians, and third parties who are responsible for TAMU-CC information resources assets.

This Control is intended to address those incident situations that escalate beyond the capability of one unit or department to handle effectively and/or have consequences potentially impacting resources outside of the unit, or if a security incident is determined to be significant (e.g., the disclosure of confidential information).

Common events like malware or other events that are detected, mitigated, and resources restored within a reasonable amount of time, with locally available unit resources, are not included in these procedures.

TAMUS Control (IR-1)

Implementation

The Chief Information Security and Privacy Officer (CISPO) shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident (e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks) as follows:

1. Develop, document, and disseminate to Owners and Custodians:
    a. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
2. Review and update the current:
    a. Incident response policy annually; and

b. Incident response procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

IR-2 Incident Response Training

Description

Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training.

For example:

i. regular users may only need to know who to call or how to recognize an incident on the information system;

ii. system administrators may require additional training on how to handle/remediate incidents; and

iii. incident responders may receive more specific training on forensics, reporting, system recovery, and restoration.

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Related Controls

- AT-3
- CP-3
- IR-8

Applicability

This Control applies to the university Chief Information Security and Privacy Officer (CISPO) and or designees who are responsible for TAMU-CC University cybersecurity incident response.

TAMUS Control (IR-2)

Implementation

TAMU-CC provides incident response training to information system users consistent with assigned roles and responsibilities:

1. Within 90 days of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. Annually thereafter.

IR-3 Incident Response Testing

Description:

Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8.

Applicability:

This control applies to the University Chief Information Security and Privacy Officer (CISPO) and or designees who are responsible for TAMU-CC University cybersecurity incident response.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall test the incident response capability for the information system at least annually using tabletop exercise to determine the incident response effectiveness and documents the results.

IR-4 Incident Handling

Description

Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems.

Incident-related information can be obtained from a variety of sources including, for example:

i. audit monitoring,
ii. network monitoring,
iii. physical access monitoring,
iv. user/administrator reports, and
v. reported supply chain events.

Effective incident handling capability includes coordination among many organizational entities including, for example:

i. mission/business owners,
ii. information system owners,
iii. authorizing officials,
iv. human resources offices,
v. physical and personnel security offices,
vi. legal departments,
vii. operations personnel,
viii. procurement offices, and
ix. the risk executive (function).

Related Controls

- AU-6
- CM-6
- CP-2
- CP-4
- IR-2
- IR-8
- PE-6
- SC-5
- SC-7
- SI-3

- SI-4

Applicability

This Control applies to all unit heads, information resource owners or custodians, and third parties who are responsible for TAMU-CC information resource assets.

This Control is intended to address those incident situations that escalate beyond the capability of one unit or department to handle effectively and/or have consequences potentially impacting resources outside of the unit or if a security incident is determined to be significant (e.g., disclosure of restricted or confidential information).

Common events like malware or other events that are detected, mitigated, and resources restored within a reasonable amount of time with locally available unit resources are not included in these procedures.

University units are responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

TAMUS Control (IR-4)

Implementation

TAMU-CC shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery as follows:

1. Documented incident handling procedures shall be developed by TAMU-CC (or by TAMU-CC and each unit that has personnel that act as custodians for information resources;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

IR-5 Incident Monitoring

Description

Documenting information system security incidents includes, for example:

i. maintaining records about each incident,

ii. the status of the incident, and

iii. other pertinent information necessary for forensics, evaluating incident details, trends, and handling.

Incident information can be obtained from a variety of sources including, for example:

i. incident reports,

ii. incident response teams,

iii. audit monitoring,

iv. network monitoring,

v. physical access monitoring, and

vi. user/administrator reports.

Related Controls

- AU-6
- IR-8
- PE-6
- SC-5
- SC-7
- SI-3
- SI-4

Applicability

This Control applies to all information resource owners and custodians, and third parties who are responsible for TAMU-CC University information resources.

The intended audience is all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security.

Common events such as malware or other events that are detected, mitigated, and resources restored within a reasonable amount of time with locally available unit resources are not included in these procedures.

TAMUS Control (IR-5)

Implementation

TAMU-CC tracks and documents information system security incidents on an ongoing basis. All users shall report all suspected information security incidents to the Service Desk.

IR-6 Incident Reporting

Description

The intent of this Control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations.

Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

Related Controls

- IR-4
- IR-5
- IR-8

Applicability

This procedure applies to all information resource owners or designees, custodians, and third parties who are responsible for TAMU-CC information resources.
Common events such as malware, or other events that are detected, mitigated, and restored within a reasonable amount of time, by locally available unit staff, are not included in this Control.
TAMUS Control (IR-6)

Implementation

The System member discloses incidents which compromise the confidentiality, integrity, or availability of major or mission-critical information systems, or systems processing confidential information, as quickly as possible upon the discovery or receipt of notification of the incident, using the notification matrix in Appendix C: Incident Notification Matrix, unless a law enforcement agency determines such a notification will impede a criminal investigation.

State Implementation

1. Security incidents shall be promptly reported to immediate supervisors and the state organization Information Security Officer. Security incidents that require timely reporting to the department include those events that are assessed to:
    a. Propagate to other state systems;
    b. Result in criminal violations that shall be reported to law enforcement; or
    c. Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information as defined in [Texas Business and Commerce Code 521.002(a)(2)], and other applicable laws that may require public notification.
2. If the security incident is assessed to involve suspected criminal activity (e.g., violations of Chapters 33, Penal Code (Computer Crimes) or Chapter 33A, Penal Code (Telecommunications Crimes)), the security incident shall be investigated, reported, and documented in a manner that restores operation promptly while meeting the legal requirements for handling of evidence.

3. Depending on the criticality of the incident, it will not always be feasible to gather all the information prior to reporting. In such cases, incident response teams should continue to report information to the department as it is collected. The department shall instruct state organizations as to the manner in which they shall report such information to the department. Supporting vendors or other third parties that report security incident information to a state organization shall submit such reports to the state organization in the form and manner specified by the department, unless otherwise directed by the state organization.
4. Summary reports of security-related events shall be sent to the department on a monthly basis no later than nine (9) calendar days after the end of the month. Organizations shall submit summary security incident reports in the form and manner specified by the department. Supporting vendors or other third parties that report security incident information to a state organization shall submit such reports to TAMU-CC in the form and manner specified by the department, unless otherwise directed by the state organization.
5. Incident Reporting using state SPECTRIM reporting system. There are two applications relating to incident reporting in the portal:
    a. Incidents – this is for individual incidents and to meet the reporting requirements associated with the urgent incident notifications. If an incident meets one or more of the following criteria you have to log the incident within 48 hours of discovery.
        i. If the incident is reported to law enforcement (i.e., typically see stolen laptops) but if law enforcement is involved in general
        ii. If it could propagate to other state systems (e.g., if you have a connection with another agency's systems and there is a potential to spread to infect them)
        iii. If it involves a breach, or suspected breach, of sensitive or confidential information.

b. Monthly incident reporting system – this is the monthly report due by the 9th of each month. It involves high level numbers about the incidents that do not meet the criteria above section 5(a).

IR-7 Incident Response Assistance

Description

Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.

Related Controls

- AT-2
- IR-4
- IR-6
- IR-8
- SA-9

Applicability

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

TAMUS Control (IR-7)

Implementation

TAMU-CC, through the Office of Information Security, provides an incident response support resource that offers advice and assistance to owners, custodians, and users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

IR-8 Incident Response Plan

Description

It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities.

As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.

Related Controls

- MP-2

Applicability

This Control applies to all TAMU-CC employees, students, information resource users, administrators, and owners, or designees. This Control also applies to all TAMU-CC assets as part of all colleges and departments whether academic or non-academic.

The applicability of this Control is not limited to person(s) or assets residing permanently or temporarily in any one state. This Control addresses, in part or whole, controls and control sets in regard to Information security monitoring, detection, and response across all federal, state, TAMU System (TAMUS), and University regulations.

TAMUS Control (IR-8)

Implementation

TAMU-CC has an incident management policy that describes the requirements for dealing with computer security incidents including prevention, detection, response, remediation, and reporting:

1. Develops an incident response plan that:
    a. Provides the organization with a roadmap for implementing its incident response capability;
    b. Describes the structure and organization of the incident response capability;

c. Provides a high-level approach for how the incident response capability fits into the overall organization;

d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

e. Defines reportable incidents;

f. Provides metrics for measuring the incident response capability within the organization;

g. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

h. Is reviewed and approved by Chief Information Security and Privacy Officer (CISPO);

2. Distributes copies of the incident response plan to the incident response team;
3. Reviews the incident response plan annually;
4. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
5. Communicates incident response plan changes to incident response team; and
6. Protects the incident response plan from unauthorized disclosure and modification.

IR-9 Information Spillage Response

Description:

Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Applicability:

This Control applies to all Texas A&M-CC information resources. The intended audience for this Control includes all owners and custodians of information resources.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall respond to information spills by:

1. Assigning Chief Information Security and Privacy Officer (CISPO) with responsibility for responding to information spills;
2. Identifying the specific information involved in the system contamination;
3. Alerting TAMUS Security Operation Center (TAMUS SOC) and Texas Department of Information Resources (DIR) of the information spill using a method of communication not associated with the spill;
4. Isolating the contaminated system or system component;
5. Eradicating the information from the contaminated system or component;
6. Identifying other systems or system components that may have been subsequently contaminated; and
7. Performing additional actions as deemed necessary by the CISPO.

Maintenance (MA) - 4 controls

MA-1 System Maintenance Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (MA-1)

Implementation

The TAMU-CC Chief Information Security and Privacy Officer shall maintain a policy that addresses system maintenance controls that shall:

1. Develop, document, and disseminate to Owners and Custodians:
    a. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Review and update the current:
    a. System maintenance policy annually; and
    b. System maintenance procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

MA-2 Controlled Maintenance

Description

This Control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers.

Information necessary for creating effective maintenance records includes, for example:

i. date and time of maintenance;
ii. name of individuals or group performing the maintenance;
iii. name of escort, if necessary;
iv. a description of the maintenance performed; and
v. information system components/equipment removed or replaced (including identification numbers, if applicable).

The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.

Related Controls

- CM-3
- CM-4
- MA-4
- MP-6
- PE-16
- SI-2

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (MA-2)

Implementation

TAMU-CC shall schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements that shall:

1. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
2. Require that Owners and Custodians explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
3. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
4. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
5. Include appropriate information in maintenance records or documented in a change control mechanism.

MA-4 Nonlocal Maintenance

Description

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication.

Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

Enforcing requirements in MA-4 is accomplished in part by other controls.

Related Controls

- AC-2
- AC-3
- AC-6
- AC-17
- AU-2
- AU-3
- IA-2
- IA-4
- IA-5
- IA-8
- MA-2
- MA-5
- MP-6
- PL-2
- SC-7

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (MA-4)

Implementation

TAMU-CC custodians shall authorize, monitor, and control any remotely executed maintenance and diagnostic activities, as follows:

1. Approve and monitor non-local maintenance and diagnostic activities;
2. Allows the use of non-local maintenance and diagnostic tools only as consistent with TAMU-CC policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for non-local maintenance and diagnostic activities; and
5. Terminates session and network connections when non-local maintenance is completed.

MA-5 Maintenance Personnel

Description

This Control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel).

Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems.

Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related Controls

- AC-2
- IA-8

- MP-2
- PE-2
- PE-3
- RA-3

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (MA-5)

Implementation

TAMU-CC allows only authorized personnel to perform maintenance on the information system, owners shall:

1. Establish a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Media Protection (MP) - 5 controls

MP-1 Media Protection Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (MP-1)

Implementation

The Chief Information Security and Privacy Officer shall maintain a policy that addresses media protection controls:

1. Develop, document, and disseminate to Owners and Custodians:
    a. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Review and update the current:
    a. Media protection policy annually; and
    b. Media protection procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

MP-2 Media Access

Description

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.

Restricting nondigital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers.

Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Related Controls

- AC-3
- IA-2
- PE-2
- PE-3
- PL-2

Applicability

This Control applies to all removable computer media managed by the university.

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

TAMUS Control (MP-2)

Implementation

TAMU-CC restricts access to confidential and controlled media to those job roles that justify the need to perform required job functions using physical access controls and safeguards.

MP-3 Media Marking

Description

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems.

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.

Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable.

Marking of information system media reflects applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

Related Controls

- PL-2
- RA-3

Applicability

This Control applies to all removable computer media managed by the university.

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

TAMUS Control (MP-3)

Implementation

TAMU-CC marks, physically or electronically, removable electronic media and information resources output containing sensitive personal information [Texas Business and Commerce Code 521.002] by indicating the ownership, distribution limitations, handling caveats, and applicable data classifications:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts controlled and confidential media from marking as long as the media remain within the Dugan data center.

MP-6 Media Sanitization

Description

This Control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices.

The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.

Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document.

NSA standards and policies control the sanitization process for media containing classified information.

Related Controls

- MA-2
- MA-4
- RA-3

Applicability

This Control applies to all information resources managed by the university.

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

TAMUS Control (MP-6)

Implementation

TAMU-CC shall:

1. Sanitize confidential and controlled system media prior to disposal, release out of organizational control, or release for reuse using data-wipe and over-write in accordance with applicable federal and organizational standards and policies, Prior to the sale or transfer of data processing equipment, to other than another Texas state agency or agent of the state, TAMU-CC shall assess whether to remove data from any associated storage device; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
    a. If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense Directive 5220.22-M: National Industrial Security Program Operating Manual [DoD 5220.22-M] standard) are provided in the "Sale or Transfer of Computers and Software" guidelines available at Texas Department of Information Resources website.

   b. Electronic state records shall be destroyed in accordance with Texas Government Code, 441.185: Record Retention Schedules [TGC 441.185]. If the record retention period applicable for an electronic state record has not
   c. expired at the time the record is removed from data process equipment, the state agency shall retain a hard copy or other electronic copy of the record for the required retention period.

3. TAMU-CC shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:
   a. date;
   b. description of the item(s) and serial number(s);
   c. inventory number(s);
   d. the process and sanitization tools used to remove the data or method of destruction; and
   e. the name and address of the organization the equipment was transferred to.

MP-7 Media Use

Description

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.

This Control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers).

In contrast to MP-2, which restricts user access to media, this Control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives.

Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media.

Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned.

Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.

Related Controls

- AC-19
- PL-4

Applicability

This Control applies to all removable computer media containing restricted or confidential university data.

The data trustee, or designee, is responsible for ensuring that the measures described in this Control are implemented.

TAMUS Control (MP-7)

Implementation

TAMU-CC shall protect confidential and controlled media types on portable media and media devices using encryption. TAMU-CC restricts the use of mobile devices with information storage capability, based on documented risk management decisions. All removable computer media containing restricted or confidential information shall have a clearly designated owner, accountable for ensuring all applicable security controls are met.

Physical and Environmental Protection (PE) - 11 controls

PE-1 Physical and Environmental Protection Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

This Control applies to facilities that house information systems (i.e., data centers) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, supervisors, managers, and others.

TAMUS Control (PE-1)

Implementation

Director of Infrastructure or his or her designated representative(s) shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification, or destruction:

1. Develop, document, and disseminate to Owners and Custodians:
    a. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
    a. Physical and environmental protection policy annually; and
    b. Physical and environmental protection procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

PE-2 Physical Access Authorizations

Description

This Control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Authorization credentials include, for example, badges, identification cards, and smart cards.

Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures.

This Control only applies to areas within facilities that have not been designated as publicly accessible.

Related Controls

- PE-3
- PS-3

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

University Unit Heads or their designees (e.g., Facility Coordinators, Area Proctors) have the responsibility for keeping an updated list of individuals with authorized access to information resource facilities.

TAMUS Control (PE-2)

Implementation

Director of Infrastructure or his or her designated representative(s) shall develop and keep current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals quarterly; and
4. Removes individuals from the facility access list when access is no longer required, within 24 hours for facilities containing information classified as restricted or confidential data and within 5 business days for other facilities containing information resources.

PE-3 Physical Access Control

Description

This Control applies to organizational employees and visitors.

Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors.

Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users.

Physical access devices include, for example, keys, locks, combinations, and card readers.

Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.

Physical access control systems comply with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems.

Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof.

Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both.

Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

Related Controls

- AU-2
- AU-6

- MP-2
- PE-2
- PS-3
- RA-3

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, facility coordinators, supervisors, managers, and others.

TAMUS Control (PE-3)

Implementation

Director of Infrastructure or his or her designated representative(s) shall control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility:

1. Enforces physical access authorizations at entry/exit points to the facility where the information system resides by;
    a. Verifying individual access authorizations before granting access to the facility; and
    b. Controlling ingress/egress to the facility using;
2. Maintains physical access audit logs for Dugan data center;

3. Provides entry access cards, video surveillance, and manual entry logs to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity when circumstances requiring visitor escorts and monitoring (e.g., entering areas that may contain controlled or confidential information);
5. Secures and maintains the inventory of keys, combinations, and other physical access devices and validates that inventory annually; and
6. Changes combinations on access cards when access cards are lost, combinations are compromised, or individuals are transferred or terminated. In cases where locks that use "Do Not Duplicate" facility keys are lost, or individuals fail to turn in during transfer or termination, those locks will be changed and keys re-issued to appropriate, authorized personnel.

PE-6 Monitoring Physical Access

Description

Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities.

Suspicious physical access activities include, for example:

i. accesses outside of normal work hours;
ii. repeated accesses to areas not normally accessed;
iii. accesses for unusual lengths of time; and
iv. out-of-sequence accesses.

Related Controls

- CA-7
- IR-4
- IR-8

Applicability

This Control applies to facilities that house moderate or high impact information resources.

TAMUS Control (PE-6)

Implementation

TAMU-CC facilities managers shall ensure audio-visual surveillance technology used to monitor physical access to information systems is used responsibly and within the intended scope of the purpose for such deployment, and transparent processes and controls are implemented for the use of such technology and any resulting recorded material:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs Quarterly and upon occurrence of events or potential indications of events; and
3. Coordinates results of reviews and investigations with the organizational incident response capability.

PE-8 Visitor Access Records

Description

Visitor access records include, for example:

i. names and organizations of persons visiting,
ii. visitor signatures,
iii. forms of identification,
iv. dates of access,
v. entry and departure times,
vi. purposes of visits, and
vii. names and organizations of persons visited.

Visitor access records are not required for publicly accessible areas.

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Physical access records shall be reviewed as needed by University Unit Heads or their designees.

TAMUS Control (PE-8)

Implementation

TAMU-CC maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible). Facility managers shall:

1. Keep logs for 365 days; and
2. Review visitor access records Quarterly.

PE-12 Emergency Lighting

Description

This Control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

Related Controls

- CP-2

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, facility coordinators, supervisors, managers, and others.

TAMUS Control (PE-12)

Implementation

TAMU-CC employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-13 Fire Protection

Description

This Control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Applicability

This Control applies to facilities that house information systems (i.e., data centers) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, supervisors, managers, and others.

TAMUS Control (PE-13)

Implementation

TAMU-CC employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Information resources shall be protected from environmental hazards. Designated employees shall monitor equipment and shall be trained in environmental control procedures and in desired response in case of emergencies or equipment problems.

PE-14 Temperature and Humidity Controls

Description

This Control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

Related Controls

- AT-3

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, facility coordinators, supervisors, managers, and others.

TAMUS Control (PE-14)

Implementation

TAMU-CC regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides:

1. Maintains temperature and humidity levels within the facility where the information system resides at acceptable levels specified by vendor recommendations; and
2. Monitors temperature and humidity levels continuously.

PE-15 Water Damage Protection

Description

This Control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

Related Controls

- AT-3

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, facility coordinators, supervisors, managers, and others.

TAMUS Control (PE-15)

Implementation

TAMU-CC protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

PE-16 Delivery and Removal

Description

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Related Controls

- CM-3
- MA-2

Applicability

This Control applies to facilities that house information systems (e.g., data centers, server rooms or closets) considered mission critical and which require a higher level of security due to the nature of one of the following:

- type of equipment
- type of data the equipment stores

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, facility coordinators, supervisors, managers, and others.

TAMUS Control (PE-16)

Implementation

TAMU-CC authorizes, monitors, and controls system components entering and exiting data processing facilities and maintains records of those items.

PE-17 Alternate Work Site

Description:

Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative.

Related controls:

AC-17, CP-7

Applicability:

Responsibility for ensuring physical security to information resources may be part of the job function for departmental staff who may include, but not be limited to, information technology staff, information resource custodians, facility coordinators, supervisors, managers, and others.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC Shall:

1. Determine and document the alternate work sites allowed for use by employees;
2. Employ equivalent security controls at alternate work sites;
3. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
4. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

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.

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 position system components within authorized facilities to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. TAMU-CC shall:

1. Consolidate all significant IT equipment into centralized approved member data center(s) or approved commercial data center.
2. The data center must have at a minimum:
    a. redundant power delivery as specified in PE-11;
    b. redundant networks as specified in CP-8;
    c. redundant cooling as specified in PE-14, and
    d. adequate physical and cybersecurity as specified in the PE and SC families.

Planning (PL) - 3 controls

PL-1 Security Planning Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (PL-1)

Implementation

The Chief Information Security and Privacy Officer (CISPO) as required by Texas Administrative Code, Chapter 202, Security Reporting [TAC 202.73(a)], delivers, at least annually, to the President/CEO a report on TAMU-CC information security program. The Chief Information Security and Privacy Officer (CISPO) shall:

1. Develop, document, and disseminate to TAMU-CC President/CEO:
    a. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
2. Review and update the current:
    a. Security planning policy annually; and
    b. Security planning procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

PL-2 System Security Plan

Description

Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements.

Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the nation if the plan is implemented as intended.

Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and

Access Management, space operations). Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist.

Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

Related Controls

- AC-2
- AC-6
- AC-14
- AC-17
- AC-20
- CA-2
- CA-3
- CA-7
- CP-2
- IR-8
- MA-4
- MA-5
- MP-2
- PM-1

- PM-7
- SA-5

Applicability

This Control is intended to apply to the university as a whole with the Department of Information Resources' "Agency Security Plan" being the "plan" indicated in this Control. (The template for this Plan is provided by the Texas Department of Information Resources (DIR) in SPECTRIM).

The university's Chief Information Security and Privacy Officer has the primary responsibility for the implementation of this Control.

However, all units in the university should make and execute security plans for the information resources they manage. These "plans" should be based on the results of risk assessments (e.g., risk management decisions and risk mitigation plans such as those provided in SPECTRIM).

TAMUS Control (PL-2)

Implementation

TAMU-CC's Chief Information Security and Privacy Officer shall develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan:

1. Develops a security plan for the information system that:
    a. Is consistent with TAMU-CC's enterprise architecture;
    b. Explicitly defines the authorization boundary for the system;
    c. Describes the operational context of the information system in terms of missions and business processes;
    d. Provides the security categorization of the information system including supporting rationale;

   e. Describes the operational environment for the information system and relationships with or connections to other information systems;
   f. Provides an overview of the security requirements for the system;
   g. Identifies any relevant overlays, if applicable;
   h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to Senior IT Leadership;
3. Reviews the security plan for the information system annually;
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

PL-4 Rules of Behavior

Description

This Control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems.

Rules of behavior for both organizational and nonorganizational users can also be established in AC-8, System Use Notification. PL-4(2) (the signed acknowledgment portion of this Control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior.

Organizations can use electronic signatures for acknowledging rules of behavior.

Related Controls

- AC-2
- AC-6
- AC-8
- AC-17
- AC-18
- AC-19
- AC-20
- AT-2
- AT-3
- CM-11
- IA-2
- IA-4
- IA-5
- MP-7
- PS-6
- PS-8
- SA-5

Applicability

This Control applies to all information resource owners, custodians, and users.

TAMUS Control (PL-4)

Implementation

TAMU-CC Office of Information Security (OIS) defines scope, behavior, and practices, compliance monitoring pertaining to users of information resources:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage. TAMU-CC documents acceptable use guidelines;
2. Ensures users formally acknowledge, agree to abide by, and adhere to prudent and responsible Internet use practices (including reasonable personal use) outlined in Texas A&M System Policy 33.04, Use of System Resources [TAMUS 33.04], and the member's acceptable use guidelines;
3. Reviews and updates the rules of behavior annually;
4. Requires individuals who have acknowledged a previous version of the rules of behavior to read and reacknowledge when the rules of behavior are revised/updated;
5. Establishes a documented process for authorization to monitor member information resources; and
6. Monitors information resources in accordance with Texas A&M System Policy 29.01, Information Resources [TAMUS 29.01].

Program Management (PM) - 12 controls

PM-1 Information Security Program Plan

Description

Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls.

Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended.

The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization.

Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems).

The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan.

If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.

Applicability

This Control applies to all information and information resources owned, leased, or under the custodianship of any unit or employee of the university, including resources outsourced to another institution, contractor, or other source such as cloud computing.

This Control provides the minimum standards for TAMU-CC's information security program in accordance with the state's Information Security Standards for Institutions of Higher Education found in Texas Administrative Code, Chapter 202 [TAC 202] and other applicable requirements.

TAMUS Control (PM-1)

Implementation

TAMU-CC is required to have an information resources security program consistent with these standards, and the Chief Information Security and Privacy Office (CISPO) is responsible for the protection of information resources as follows:

1. Develop and disseminates an organization-wide information security program plan that:
    a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    c. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
    d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation;
2. Review the organization-wide information security program plan annually;
3. Update the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
4. Protect the information security program plan from unauthorized disclosure and modification.

PM-2 Senior Information Security Officer

Description

The security officer described in this Control is an organizational official.

For a federal agency (as defined in applicable federal laws, executive orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

Applicability

This Control describes the authority and responsibilities (including but not limited to) for TAMU-CC's Chief Information Security and Privacy Officer (CISPO).

TAMUS Control (PM-2)

Implementation

TAMU-CC appoints a Chief Information Security and Privacy Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

PM-3 Information Security Resources

Description

Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.

Related Controls

- PM-4
- SA-2

Applicability

This Control applies to the University Vice President for Information Technology and Chief Information Officer (CIO) working in cooperation with university administrative management and the University Chief Information Security and Privacy Officer (CISPO). TAMUS Control (PM-3)

Implementation

TAMU-CC's Vice President for Information Technology and Chief Information Officer (CIO) shall:

1. Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
2. Employ a business case/Exhibit 300/Exhibit 53 to record the resources required;
3. Ensure that information security resources are available for expenditure as planned; and
4. Implement this standard as incorporated into Texas Administrative Code, Chapter 202 [TAC 202].

PM-4 Plan of Action and Milestones Process

Description

The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB.

With the increasing emphasis on organization wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization.

Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

Related Controls

- CA-5

Applicability

Texas Administrative Code, Chapter 202 [TAC 202] assigns responsibility for the protection of information resources to the President of the University.

For the purposes of this Control, the authority and responsibility regarding the university's compliance with TAC 202 have been delegated by the President to the Chief Information Officer (CIO).

TAMUS Control (PM-4)

Implementation

TAMU-CC develops and updates, a plan of action and milestone process for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls in order to reduce or eliminate known vulnerabilities in the system:

1. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
    a. Are developed and maintained;
    b. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the nation; and
    c. Are reported in accordance with OMB FISMA reporting requirements.
2. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-5 Information System Inventory

Description

This Control addresses the inventory requirements in FISMA.

OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

Applicability

The authority and responsibility regarding the university's compliance with Texas Administrative Code, Chapter 202 [TAC 202] have been delegated by the President to the Chief Information Officer (CIO).

TAMUS Control (PM-5)

Implementation

TAMU-CC develops and maintains an inventory of its information systems, as follows:

1. Designates a single system of record for inventory of all information systems owned or managed by the member;
2. Includes any cloud computing services [SP 800-145] operated by the member in its inventory of information systems, and
3. Designates which data regarding an information system to record in the inventory of information systems. At a minimum, the data includes a unique identifier (e.g., serial number or system name), owner, custodian, and highest level of data classification stored/processed on the information system.

PM-6 Information Security Measures of Performance

Description

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Applicability

Texas Administrative Code, Chapter 202 [TAC 202] assigns responsibility for the protection of information resources to the President of the University.

For the purposes of this Control, the authority and responsibility regarding the university's compliance with TAC 202 have been delegated by the President to the Chief Information Security and Privacy Officer (CISPO), under the supervision of the Senior Associate Vice President for Information Technology/Chief Information Officer (CIO). (TAMU-CC Rule 29.01.99.C1, Security of Electronic Information Resources [TAMU-CC 29.01.99.C1])

TAMUS Control (PM-6)

Implementation

TAMU-CC's Chief Information Security and Privacy Officer shall develop, monitor, and report on the results of information security measures of performance in an annual risk assessment, containing a Risk Management Plan.

PM-7 Enterprise Architecture

Description

The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture.

The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes.

This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies.

For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems.

The information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization.

Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines.

The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.

Related Controls

- PL-2
- RA-2
- SA-3

Applicability

Texas Administrative Code, Chapter 202 [TAC 202] assigns responsibility for the protection of information resources to the President of the University.

For the purposes of this Control, the authority and responsibility regarding the university's compliance with TAC 202 have been delegated by the President to the Chief Information Officer (CIO).

TAMUS Control (PM-7)

Implementation

TAMU-CC shall develop an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation. The TAMU-CC implementation of this standard is an outcome of TAC 202 implementation.

PM-9 Risk Management Strategy

Description:

An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

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: (delay effective date: 07/20/2023)

TAMU-CC shall:

1. Develops a comprehensive strategy to manage:
    a. Security risk to organizational operations and assets, individuals, other organizations, the State of Texas, and the Nation associated with the operation and use of organizational systems; and
    b. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
2. Implement the risk management strategy consistently across the organization; and
3. Review and update the risk management strategy annually or as required, to address organizational changes.

PM-10 Authorization Process

Description:

Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and the Nation.

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: (delay effective date: 07/20/2023)

TAMU-CC shall:

1. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
2. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
3. Integrate the authorization processes into an organization-wide risk management program.

PM-14 Testing, Training, Monitoring

Description

A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Related Controls

- AT-3
- CA-7
- CP-4
- SI-4

Applicability

Texas Administrative Code Chapter202 assigns responsibility for the protection of information resources to the President of the University.

For the purposes of this Control, the authority and responsibility regarding the university's compliance with TAC 202 have been delegated by the President to the Chief Information Officer (CIO)

Implementation

TAMU-CC shall ensure an IT organization is designated to provide security monitoring for all information systems, in both centralized and decentralized (distributed) IT environments, owned or managed by the University.

1. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
    a. Are developed and maintained; and

   b. Continue to be executed in a timely manner;

2. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
3. Ensure an IT organization is designated to provide security monitoring for all information systems, in both centralized and decentralized IT environments, owned or managed by the organization.

PM-15 Security and Privacy Groups and Associations

Description:

Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations share threat, vulnerability, and incident information as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidelines.

Applicability:

This control applies to the university Chief Information Security and Privacy Officer (*CISPO*).

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall establish and institutionalize contact with selected groups and associations within the security and privacy communities:

1. To facilitate ongoing security and privacy education and training for organizational personnel;
2. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
3. To share current security and privacy information, including threats, vulnerabilities, and incidents.

PM-16 Threat Awareness Program

Description

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems.

One of the best techniques to address this concern is for organizations to share threat information. This can include, for example:

i. sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced,

ii. mitigations that organizations have found are effective against certain types of threats, and

iii. threat intelligence (i.e., indications and warnings about threats that are likely to occur).

Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia).

Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

Applicability

Texas Administrative Code, Chapter 202 [TAC 202] assigns responsibility for the protection of information resources to the President of the University.

For the purposes of this Control, the authority and responsibility regarding the university's compliance with TAC 202 have been delegated by the President to the Chief Information Officer (CIO).

TAMUS Control (PM-16)

Implementation

TAMU-CC implements a threat awareness program that includes a cross-organization information sharing capability. Administering an ongoing information security awareness education program for all users; and Introducing information security awareness and informing new employees of information security policies and procedures during the onboarding process. TAMU-CC implementation of this standard is incorporated into TAC 202.

Personnel Security (PS) - 8 controls

PS-1 Personnel Security Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (PS-1)

Implementation

The Chief Information Security and Privacy Officer has a formal, documented, personnel security policy as follows:

1. Develop, document, and disseminate to Owners and Custodians:
    a. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
    a. Personnel security policy annually; and
    b. Personnel security procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

PS-2 Position Risk Designation

Description

Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems.

Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).

Related Controls

- AT-3
- PL-2
- PS-3

Applicability

This Control applies to all information system owners and managers.

TAMUS Control (PS-2)

Implementation

All authorized users (including, but not limited to, state organization personnel, temporary employees, and employees of independent contractors) of the state organization's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the state organization or they shall not be granted access to information resources. The head of TAMU-CC personnel management, or his or her designated representative, will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to state organization information resources.

TAMU-CC resource owner or custodians, in conjunction with Human Resource shall:

1. Assigns a risk designation to all organizational positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and updates position risk designations annually.

PS-3 Personnel Screening

Description

Personnel screening and rescreening activities reflect applicable federal laws, executive orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

Related Controls

- AC-2
- IA-4
- PE-2
- PS-2

Applicability

This Control applies to all information resource owners and unit managers.

TAMUS Control (PS-3)

Implementation

TAMU-CC shall screen individuals requiring access to organizational information and information systems before authorizing access.

It is the responsibility of the information resource owner or custodian, in conjunction with Human Resources, to:

1. Screen individuals prior to authorizing access to the information system; and
2. Rescreen individuals according to the unit's human resource policies.

PS-4 Personnel Termination

Description

Information system-related property includes, for example:

i. hardware authentication tokens,
ii. system administration technical manuals,
iii. keys,
iv. identification cards, and
v. building passes.

Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment.

Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors.

Exit interviews are important for individuals with security clearances.

Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.

Related Controls

- AC-2
- IA-4
- PE-2
- PS-5
- PS-6

Applicability

This Control applies to all information resource owners and unit managers.

TAMUS Control (PS-4)

Implementation

TAMU-CC terminates information system access, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems. TAMU-CC owners and unit managers, in conjunction with Human Resources, upon termination of individuals employment shall:

1. Disable information system access within 72 hours of the individuals last day or as directed by individual's supervisor and/or Human Resources;
2. Terminate/revoke any authenticators/credentials associated with the individual;
3. Conduct exit interviews that include a discussion of related information security topics;
4. Retrieve all security-related organizational information system-related property;
5. Retain access to organizational information and information systems formerly controlled by terminated individual; and
6. Human Resources will notify the "separating employee distribution" e-mail group with termination date and individuals' information by the individuals last day of employment.

PS-5 Personnel Transfer

Description

This Control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example:

i. returning old and issuing new keys, identification cards, and building passes;

ii. closing information system accounts and establishing new accounts;

iii. changing information system access authorizations (i.e., privileges); and

iv. providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

Related Controls

- AC-2
- IA-4
- PE-2
- PS-4

Applicability

This Control applies to all information resource owners and unit managers.

TAMUS Control (PS-5)

Implementation

TAMU-CC owners and unit managers, in conjunction with Human Resources, review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

2. Hiring manager initiates reassignment actions within for new user right and the former manager initiates terminates unneeded access. The effective date shall be within the transfer date of the employee or an alternative date agreed to by both hiring manager and former manager;
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies Identity management within 72 hours.

PS-6 Access Agreements

Description

Access agreements include, for example:

i. nondisclosure agreements,
ii. acceptable use agreements,
iii. rules of behavior, and
iv. conflict-of-interest agreements.

Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized.

Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related Controls

- PL-4
- PS-2
- PS-3
- PS-4
- PS-8

Applicability

This Control applies to the Chief Information Officer (CIO).

TAMUS Control (PS-6)

Implementation

TAMU-CC shall complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access as follows:

1. Develop and document access agreements for organizational information systems;
2. Reviews and updates the access agreements before access is granted; and
3. Ensures that individuals requiring access to organizational information and information systems:
    a. Sign appropriate access agreements prior to being granted access; and
    b. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or every four (4) years.

PS-7 Third-party Personnel Security

Description

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

Organizations explicitly include personnel security requirements in acquisition-related documents.

Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations.

Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials.

Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

Related Controls

- PS-2
- PS-3
- PS-4
- PS-5
- PS-6
- SA-9

Applicability

This Control applies to all information resource owners and unit managers.

TAMUS Control (PS-7)

Implementation

TAMU-CC establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify contract owner of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within 72 hours; and
5. Monitors provider compliance.

PS-8 Personnel Sanctions

Description

Organizational sanctions processes reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations.

Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related Controls

- PL-4
- PS-6

Applicability

This Control applies to the university Chief Information Officer (CIO).

TAMUS Control (PS-8)

Implementation

TAMU-CC employs a formal sanctions process for personnel failing to comply with established information security policies and procedures as follows:

1. Employs procedure " TAMU-CC Acceptable Use Policy, Acceptable Use, Section 1 and IT Privacy, Section 2" as the formal sanctions process for individuals failing to comply with established information security policies and procedures; and
2. Procedure " TAMU-CC Acceptable Use Policy, Acceptable Use, Section 1 and IT Privacy, Section 2" and related University policy outlines procedures when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Personally Identifiable Information Processing and Transparency (PT) - 2 controls

PT-1 Policy and Procedures

Description:

Personally identifiable information processing and transparency policy and procedures address the controls in the PT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of personally identifiable information processing and transparency policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to personally identifiable information processing and transparency policy and procedures include assessment or audit findings, breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Applicability:

This control applies to the university Chief Information Security and Privacy Officer.

Implementation: (delay effective date: 08/01/2022)

TAMU-CC Shall:

1) Develop, document, and disseminate to owners, custodians, faculty, and staff:
    a) personally identifiable information processing and transparency policy that:
        i) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    ii) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

  b) Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

2) Designate an official to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

3) Review and update the current personally identifiable information processing and transparency:

  a) Policy annually and following privacy related security events; and

  b) Procedures annually and following privacy related security events.

PT-3 Personally Identifiable Information Processing Purposes

Description:

Identifying and documenting the purpose for processing provides organizations with a basis for understanding why personally identifiable information may be processed. The term Organizations take steps to help ensure that personally identifiable information is processed only for identified purposes, including training organizational personnel and monitoring and auditing organizational processing of personally identifiable information. Organizations monitor for changes in personally identifiable information processing. Organizational personnel consult with the senior agency official for privacy and legal counsel to ensure that any new purposes that arise from changes in processing are compatible with the purpose for which the information was collected, or if the new purpose is not compatible, implement mechanisms in accordance with defined requirements to allow for the new processing, if appropriate. Mechanisms may include obtaining consent from individuals, revising privacy policies, or other measures to manage privacy risks that arise from changes in personally identifiable information processing purposes.

Applicability:

This control applies to all information Owners and Custodians.

Implementation: (delay effective date: 08/01/2022)

TAMU-CC Shall:

1) Identify and document the purpose(s) for processing personally identifiable information;
2) Describe the purpose(s) in the public privacy notices and policies of the organization;
3) Restrict the processing of personally identifiable information to only that which is compatible with the identified purpose(s); and
4) Monitor changes in processing personally identifiable information and implement mechanisms to ensure that any changes are made In accordance with federal laws, executive orders, directives, policies, regulations, standards, and/or guidance.
5) Reduce, and eliminate where possible, the collection and/or use of sensitive personal information [TxBCC 521.002] in information resources under the control of the organization.

Risk Assessment (RA) - 6 controls

RA-1 Risk Assessment Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (RA-1)

Implementation

Chief Information Security and Privacy Officer has a risk assessment policy which includes process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on TAMU-CC's mission, functions, image, reputation, assets, or individuals:

1. Develops, documents, and disseminates to Owners and Custodians:
    a. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
    a. Risk assessment policy annually; and
    b. Risk assessment procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

RA-2 Security Categorization

Description

Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions.

Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability.

Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards.

Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts.

Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.

Related Controls

- CM-8
- RA-3
- SC-7

Applicability

This Control applies to all information resource owners, custodians, and users. It also applies to information resources storing University Data regardless of ownership of the particular storage device. Other federal, state, or contractual requirements may be more restrictive than the procedures specified in this Control (example: Classified National Security Information). In no situation can procedures regarding security of data be less restrictive than this Control, regardless of the contract or agreement specifications.

TAMUS Control (RA-2)

Implementation

TAMU-CC categorizes information and information systems owned or managed by the University using a data classification structure that incorporates the guidance provided in in the Texas A&M University System Data Classification Standard, Appendix D [TAMUS Data Classification], at a minimum:

1. Categorizes information and the information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-3 Risk Assessment

Description

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the nation based on the operation and use of information systems.

Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).

In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.

Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation , security control assessment, information system authorization, and security control monitoring.

RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework.

Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.

Related Controls

- RA-2

Applicability

This Control applies to all information security risk assessments that are conducted annually for university information resources.

The intended audience includes all University personnel involved in performing, assisting with, approving, or making risk management decisions related to information security risk assessments

TAMUS Control (RA-3)

Implementation

TAMU-CC:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. A risk assessment of information resources shall be performed and documented. The risk assessment shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," "Moderate," or "Low.";
2. Documents risk assessment results in annual report to the University President/CEO. Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the state organization head or his or her designated representative(s). The state organization head or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The state organization head or his or her designated representative(s) shall approve the security risk management plan. This information may be exempt from disclosure under Texas Government Code, 2054.077: Vulnerability Reports [TGC 2054.077(c)];
3. Reviews risk assessment results annually;
4. Disseminates risk assessment results to Chief Information Officer (CIO) and the University President/CEO; and
5. Updates the risk assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3(1) Supply Chain Risk Assessment

Description:

Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Applicability:

This Control applies to all information security risk assessments that are conducted annually for university information resources.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall:

1. Assess supply chain risks associated with systems, components, and services; and
2. Update the supply chain risk assessment annually, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

RA-5 Vulnerability Scanning

Description

Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans.

Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked.

Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews.

Vulnerability scanning includes, for example:

i. scanning for patch levels;

ii. scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and

iii. scanning for improperly configured or incorrectly operating information flow control mechanisms.

Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Related Controls

- CA-2
- CA-7
- CM-4
- CM-6
- RA-2
- RA-3
- SI-2

Applicability

A Unit head, or designee, will ensure that all information resources that connect to the University’s network undergo periodic security vulnerability assessments conducted centrally by the University's Division of Information Technology.

TAMUS Control (RA-5)

Implementation

TAMU-CC Office of Information Security (OIS) scans for vulnerabilities in the information system at least annually or when significant new vulnerabilities potentially affecting the system are identified and reported:

1. Scans for vulnerabilities in the information system and hosted applications servers monthly and workstations weekly and when new vulnerabilities potentially affecting the system/applications are identified and reported;
2. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    a. Enumerating platforms, software flaws, and improper configurations;
    b. Formatting checklists and test procedures; and
    c. Measuring vulnerability impact;
3. Analyzes vulnerability scan reports and results from security control assessments;
4. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk.
    a. For vulnerabilities with a Severity of Critical, High or Important: within 30 days either 1) remediate the vulnerability or 2) send a written exception request to OIS containing the IRIS keys of the relevant resources and a rationale for the exception and mitigating controls put in place.
    b. For all other vulnerabilities, decide whether and when to remediate based upon a risk assessment; and
5. Shares information obtained from the vulnerability scanning process and security control assessments with Custodian to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-7 Risk Response

Description:

Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing, or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and milestones entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

Applicability:

This Control applies to all information security risk assessments that are conducted annually for university information resources

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

System and Services Acquisition (SA) - 10 controls

SA-1 System and Services Acquisition Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed.

The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (SA-1)

Implementation

Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources by the university Chief Information Security and Privacy Officer (CISPO) and in coordination with Information Resource owners as follows:

1. Develop, document, and disseminate to TAMU-CC Faculty, Staff, and Researchers:
    a. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Review and update the current:
    a. System and services acquisition policy annually; and
    b. System and services acquisition procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

SA-2 Allocation of Resources

Description

Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.

Related Controls

- PM-3

Applicability

The University is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (SA-2)

Implementation

In accordance with Texas Administrative Code 202.70, Responsibilities of the Institution Head [TAC 202.70], TAMU-CC University is responsible for:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

SA-3 System Development Life Cycle

Description

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions.

The security engineering principles in SA-8 [Texas DIR, page 150] cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems.

It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes.

This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.

Related Controls

- AT-3
- PM-7

Applicability

The unit head or information resource owner is responsible for ensuring that all requirements of this Control are substantiated and maintained throughout the life cycle of an information system.

TAMUS Control (SA-3)

Implementation

Chief Information Security and Privacy Officer (CISPO) reviews the data security requirements and specifications of any new information systems or services that process and/or store sensitive or mission critical information to:

1. Manage the information system using the TAMU-CC system development life cycle that incorporates information security considerations. Additionally, Information security, security testing, and audit controls shall be included in all phases of the system development lifecycle or acquisition process;
2. Define and document information security roles and responsibilities throughout the system development life cycle;
3. Identify individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

SA-4 Acquisition Process

Description

Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system.

Information system components include commercial information technology products.

Security functional requirements include security capabilities, security functions, and security mechanisms.

Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass.

Security assurance requirements include:

i. development processes, procedures, practices, and methodologies; and

ii. evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved.

Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process.

The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information.

Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy).

Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services.

Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement.

The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.

Related Controls

- CM-6
- PL-2
- PS-7
- SA-3

- SA-5

Applicability

This Control applies to any university personnel who currently have, or will have, a vendor, third party or cloud computing service provider agreement or contract.

The procedures in this Control shall be applied to new contracts or agreements, renewal of existing contracts or agreements, and amendments to existing contracts or agreements. Information resources contracts must include all terms required in this Control.

TAMUS Control (SA-4)

Implementation

TAMU-CC includes the following security requirements and/or security specifications, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs.

The Chief Information Security and Privacy Officer (CISPO):

1. Reviews and approves the security requirements in acquisition contracts of any new information system that processes and/or stores sensitive or mission-critical information prior to the member procuring the system or service to validate and ensure:
    a. Security functional requirements;
    b. Security strength requirements;
    c. Security assurance requirements;
    d. Security-related documentation requirements;
    e. Requirements for protecting security-related documentation;
    f. Description of the information system development environment and environment in which the system is intended to operate; and
    g. Acceptance criteria.

2. Ensures acquisition contracts for information systems, system components, or information system services address information security, backup, and privacy requirements:
    a. Such contracts should include right-to-audit and other provisions to provide appropriate assurance that applications and information are adequately protected.
    b. Vendors and third parties adhere to all state and Federal laws and System policies pertaining to the protection of information resources and privacy of sensitive information.

SA-5 Information System Documentation

Description

This Control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services.

Organizations consider establishing specific measures to determine the quality/completeness of the content provided.

The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls.

The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system.

Documentation that addresses information system vulnerabilities may also require an increased level of protection.

Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

Related Controls

- CM-6
- CM-8
- PL-2
- PL-4
- PS-2
- SA-3
- SA-4

Applicability

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (SA-5)

Implementation

TAMU-CC obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   a. Secure configuration, installation, and operation of the system, component, or service;
   b. Effective use and maintenance of security functions/mechanisms; and
   c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   a. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

   b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   c. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to Owners, Custodians, and Users.

SA-8 Security Engineering Principles

Description:

Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Applicability:

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

SA-9 External Information System Services

Description

External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems.

FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet.

Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges.

The responsibility for managing risks from the use of external information system services remains with authorizing officials.

For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time.

External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related Controls

- CA-3
- IR-7
- PS-7

Applicability

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (SA-9)

Implementation

TAMU-CC requires that providers of external information system services employ adequate security controls in accordance with these standards and monitors security control compliance. The information resource owner, or designee, is responsible for:

1. Requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. (E.g., annual Risk Assessments).

SA-10 Developer Configuration Management

Description

This Control also applies to organizations conducting internal information systems development and integration.

Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware.

Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Configuration items that are placed under configuration management (if existence/use is required by other security controls) include:

i. the formal model;
ii. the functional, high-level, and low-level design specifications;
iii. other design data;
iv. implementation documentation;
v. source code and hardware schematics;
vi. the running version of the object code;
vii. tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and
viii. test fixtures and documentation.

Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.

Related Controls

- CM-3
- CM-4
- SI-2

Applicability

The intended audience includes developers, custodians and/or owners of an information resource.

TAMUS Control (SA-10)

Implementation

All security-related information resources changes shall be approved by the information owner through a change control process. Approval shall occur prior to implementation by TAMU-CC or independent contractors. TAMU-CC requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service design, development, implementation, or operation;
2. Document, manage, and control the integrity of configuration changes using TAMU-CC's change management process;
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to Office of Information Security (OIS).

SA-11 Developer Security Testing and Evaluation

Description:

Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

Related controls:

CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Applicability:

The intended audience includes developers, custodians and/or owners of an information resource.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall require the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform testing/evaluation;

3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

SA-22 Unsupported System Components

Description:

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks, or implementing other forms of isolation.

Applicability:

The owner of an information resource, or designee, is responsible for implementing this control.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall:

1. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
2. Provide the following options for alternative sources for continued support for unsupported components:
    a. In-house support where appropriate
    b. External providers where available

System and Communications Protection (SC) - 11 controls

SC-1 System and Communications Protection Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (SC-1)

Implementation

The Chief Information Security and Privacy Officer shall:

1. Develop, document, and disseminate to Owners and Custodians:
    a. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Review and update the current:
    a. System and communications protection policy annually; and
    b. System and communications protection procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

SC-5 Denial of Service Protection

Description

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial-of-service attacks. For example, boundary protection devices can filter certain types of

packets to protect information system components on internal organizational networks from being directly affected by denial-of-service attacks.
Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial-of-service attacks.

Related Controls

- SC-7

Applicability

This Control applies to all TAMU-CC network information resources. The intended audience for this Control includes all information resource owners and custodians.
TAMUS Control (SC-5)

Implementation

The information system protects against or limits the effects of the following types of denial-of-service attacks. The Director of Infrastructure or his/her designated representative and The Chief Information Security and Privacy Officer (CISPO) shall:

1. Establish a security strategy that includes perimeter protection.
2. Provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize state information resources as specified in Texas Government Code, Chapter 2054, Information Resources [TGC 2054] and Chapter 2059, Texas Computer Network Security System [TGC 2059]. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router.

SC-7 Boundary Protection

Description

Managed interfaces include, for example:

i. gateways,
ii. routers,

iii. firewalls,

iv. guards,

v. network-based malicious code analysis and virtualization systems, or

vi. encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs.

Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

Related Controls

- AC-17
- CA-3
- CM-7
- IR-4
- RA-3
- SC-5
- SC-13

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee, is responsible for implementing this Control.

TAMUS Control (SC-7)

Implementation

The Chief Information Security and Privacy Officer (CISPO), or designee, is responsible for:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
2. Implements subnetworks for publicly accessible system components that are separated from internal organizational networks; and
3. Ensuring connects to external networks or information systems are only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

SC-8 Transmission Confidentiality and Integrity

Description

This Control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques).

Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages.

If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

Related Controls

- AC-17

Applicability

This Control applies to all TAMU-CC information resources. The intended audience is all users of university information resources.

TAMUS Control (SC-8)

Implementation

The information system protects the confidentiality and integrity of transmitted information. Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted with, at minimum a 128-bit encryption algorithm. Implementing encryption for other data classifications where prudent is encouraged.

SC-12 Cryptographic Key Establishment and Management

Description

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures.

Organizations define key management requirements in accordance with applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters.

Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.

Related Controls

- SC-13

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (SC-12)

Implementation

Information resource owner, or designee shall:

1. Establishes and manages cryptographic keys for required cryptography employed within the information system. When cryptography is required and employed within the information system, TAMU-CC; and
2. Establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

SC-13 Cryptographic Protection

Description

Cryptography can be employed to support a variety of security solutions including, for example:

i. the protection of classified and Controlled Unclassified Information,
ii. the provision of digital signatures, and
iii. the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

Cryptography can also be used to support random number generation and hash generation.

Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography.

This Control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

Related Controls

- AC-2
- AC-3
- AC-7
- AC-17
- AC-18
- AU-9
- CM-11
- CP-9
- IA-7
- MA-4
- MP-2
- SA-4
- SC-8
- SC-12

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (SC-13)

Implementation

The information system ensures that information systems owned or operated by the university implement FIPS-validated cryptography [FIPS 140-2] in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards.

1. Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management, shall be based on documented TAMU-CC University risk management decisions.
2. Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted.
3. Confidential information and protected data types stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted.
4. Storing confidential information on portable devices is discouraged. Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-TAMU-CC owned computing device.
5. The minimum algorithm strength for protecting confidential information is a 128-bit encryption algorithm, subject to state organization risk management decisions justified and documented in accordance with Texas Administrative Code, Chapter 202, Responsibilities of the Information Security Officer [TAC 202.71(c)] and Managing Security Risks [TAC 202.75].
6. A TAMU-CC may also choose to implement additional protections, such as, but not limited to, stronger encryption algorithms or key lengths, based upon risk management decisions.

SC-15 Collaborative Computing Devices

Description

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (SC-15)

Implementation

The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users, as follow:

1. Prohibits remote activation of collaborative computing devices that have exceptions on file with the Office of Information Security; and
2. Provides an explicit indication of use to users physically present at the devices.

SC-20 Secure Name / Address Resolution Service (Authoritative Source)

Description

This Control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys.

DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS.

The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23.

Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related Controls

- SC-8
- SC-12
- SC-13
- SC-21
- SC-22

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee, is responsible for implementing this Control.

TAMUS Control (SC-20)

Implementation

The Chief Information Security and Privacy Officer (CISPO), or designee, is responsible for ensuring procedures are in place that:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

Description

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers.

Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.
Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

Related Controls

- SC-20
- SC-22

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee, is responsible for implementing this Control.

TAMUS Control (SC-21)

Implementation

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

SC-22 Architecture and Provisioning for Name / Address Resolution Service

Description

Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.
To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server

and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility).

For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet).

Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

Related Controls

- SC-20
- SC-21

Applicability

The Chief Information Security and Privacy Officer (CISPO), or designee, is responsible for implementing this Control.

TAMUS Control (SC-22)

Implementation

The information systems that collectively provide name/address resolution service for TAMU-CC are fault tolerant and implement internal/external role separation.

SC-39 Process Isolation

Description

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space.

Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multistate processor technologies.

Related Controls

- AC-3
- AC-6
- SA-4
- SA-5

Applicability

The owner of an information resource, or designee, is responsible for implementing this Control.

TAMUS Control (SC-39)

Implementation

TAMU-CC shall use operating systems that support process isolation. The information system maintains a separate execution domain for each executing process.

System and Information Integrity (SI) - 6 controls

SI-1 System and Information Integrity Policy and Procedures

Description

This Control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary.

The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations.

The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Applicability

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

TAMUS Control (SI-1)

Implementation

The integrity of data, its source, its destination, and processes applied to it shall be assured. Changes to data shall be made only in an authorized manner. Chief Information Security and Privacy Officer shall:

1. Develop, document, and disseminate to Owners and Custodians:
    a. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
    a. System and information integrity policy annually; and
    b. System and information integrity procedures annually or when required by information systems, TAMU System, state, federal, and/or regulatory requirements change.

SI-2 Flaw Remediation

Description

Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities.

Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.

Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling.

Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems.

By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).

Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related Controls

- CA-2
- CA-7
- CM-3
- CM-8
- MA-2
- IR-4
- RA-5
- SA-10

Applicability

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (SI-2)

Implementation

TAMU-CC Shall:

1. Identify, report, and correct information system flaws;
2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Install security-relevant software and firmware updates within 30 days of the release of the updates; and
4. Incorporate flaw remediation into the organizational configuration management process.

SI-3 Malicious Code Protection

Description

Information system entry and exit points include, for example:

i. firewalls,

ii. electronic mail servers,

iii. web servers,

iv. proxy servers,

v. remote-access servers,

vi. workstations,

vii. notebook computers, and

viii. mobile devices.

Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography.

Malicious code can be transported by different means including, for example:

i. web accesses,

ii. electronic mail,

iii. electronic mail attachments, and

iv. portable storage devices.

Malicious code insertions occur through the exploitation of information system vulnerabilities.

Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code.

In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to:

i. malicious code detection during periodic scans,
ii. actions in response to detection of malicious downloads, and/or
iii. actions in response to detection of maliciousness when attempting to open or execute files.

Related Controls

- CM-3
- MP-2
- SA-4
- SC-7
- SI-2
- SI-4

Applicability

This Control applies to all TAMU-CC information resources.

The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

TAMUS Control (SI-3)

Implementation

TAMU-CC implements malicious code protection:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:

   a. Perform periodic scans of the information system monthly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with TAMU-CC's security policy; and
   b. In response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
5. Ensures all System-owned or -managed information systems that connect to a member network employ endpoint protection software and any other protective measures required by applicable policies or guidelines, and
6. Ensures personally owned devices that connect to networks within the same boundary as confidential or mission-critical information systems employ endpoint protection software or suitable compensating controls, based on assessed risk.

SI-4 Information System Monitoring

Description

Information system monitoring includes external and internal monitoring.

External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system.

Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events.

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software).

Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices.

The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies.

Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs.

A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Related Controls

- AC-3
- AC-8
- AC-17
- AU-2
- AU-6
- AU-9
- AU-12
- CA-7
- IR-4
- PE-3
- RA-5
- SC-7

- SI-3

Applicability

This Control applies to all university managed information resources containing mission critical information, confidential information, and other information resources as may be managed by TAMU-CC.

The purpose of the implementation of this Control is to provide a set of measures that will mitigate information security risks associated with security monitoring. There may be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

The intended audience is all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security.

TAMUS Control (SI-4)

Implementation

Chief Information Officer (CIO) or his/her designated representative and Chief Information Security and Privacy Officer shall establish a security strategy that includes perimeter protection. TAMU-CC ensures the security of information systems through monitoring network traffic and use of information resources:

1. Monitors the information system to detect:
    a. Attacks and indicators of potential attacks in accordance with alerts from monitoring devices and services; and
    b. Unauthorized local, network, and remote connections;

2. The Office of Information Security will provide security information management services to include external network monitoring, scanning, and alerting for TAMU-CC that utilize TAMU-CC information resources as specified in Texas Government Code, Chapter 2054, Information Resources [TGC 2054] and Chapter 2059, Texas Computer Network Security System [TGC 2059]. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router.
3. Identifies unauthorized use of the information system through alerts generated by monitoring devices and services;
4. Deploys monitoring devices:
    a. Strategically within the information system to collect organization-determined essential information; and
    b. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
5. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
6. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information;
7. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, executive orders, directives, policies, or regulations; and
8. Provides alerts and status updates to Owners and Custodians of Information Resources.

SI-5 Security Alerts, Advisories, and Directives

Description

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives.

Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the nation should the directives not be implemented in a timely manner.

External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

Related Controls

- SI-2

Applicability

Security alerts, advisories, and directives are the responsibility of the Chief Information Security and Privacy Officer (CISPO).

TAMUS Control (SI-5)

Implementation

TAMU-CC:

1. Receives information system security alerts, advisories, and directives from DIR Office of the Chief Information Security Officer, REN-ISAC, and other information security resources on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to owners and custodians of related information resources; and
4. Implements security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance.

State Implementation

The state organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

SI-12 Information Handling and Retention

Description

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.

Related Controls

- AU-5
- AU-11
- MP-2

Applicability

This Control applies to all TAMU-CC information resources.

The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

The information resource owner, or designee, is responsible for ensuring that all requirements of this Control are satisfied.

TAMUS Control (SI-12)

Implementation

TAMU-CC information resource owners, custodians, and users are required to handle and retain information within the information system and information output from the system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and operational requirements.

SI-10 Information Input Validation

Description:

Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

Applicability:

This Control applies to all TAMU-CC information resources.

The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall check the validity of information inputs in automated systems.

Supply Chain Risk Management (SR)- 6 controls

SR-1 Policy and Procedures

Description:

Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Applicability:

This control applies to the university Chief Information Security and Privacy Officer (*CISPO*).

Implementation: (delay effective date: 07/20/2023)

TAMU-CC Shall:

1. Develop, document, and disseminate to Owners and custodians:
    a. Supply chain risk management policy that:
        i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

        ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    b. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;
2. Designate an official to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and
3. Review and update the current supply chain risk management:
    a. Policy annually; and
    b. Procedures annually.

SR-2 Supply Chain Risk Management Plan

Description:

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions. Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk 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 plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Applicability:

The owner of an information resource, or designee, is responsible for implementing this control.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC Shall:

1) Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of systems, system components or system services;
2) Implement the supply chain risk management plan consistently across the organization; and
3) Review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes.

SR-3 Supply Chain Controls and Processes

Description:

Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.

Applicability:

The owner of an information resource, or designee, is responsible for implementing this control.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC Shall:

1) Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of system components in coordination with supply chain personnel;
2) Employ supply chain controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events; and
3) Document the selected and implemented supply chain processes and controls in
    a) security and privacy plans

b) supply chain risk management plan

SR-5 Strategies, Tools, and Methods

Description:

The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Applicability:

The owner of an information resource, or designee, is responsible for implementing this control.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

SR-8 Notification Agreements

Description:

The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Applicability:

The owner of an information resource, or designee, is responsible for implementing this control.

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the:

1) notification of supply chain compromises; and
2) results of assessments or audits

SR-12 Component Disposal

Description:

Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

Applicability:

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

Implementation: (delay effective date: 07/20/2023)

TAMU-CC shall dispose of *data, documentation, tools, and system components* using the following techniques and methods:

1. *Data sanitization*
2. *Shredding*
3. *Secure third party services*

Data Minimization and Retention (DM) - 1 control

DM-1 Minimization of Personally Identifiable Information

Description

Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials consult with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete.

Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose.

OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.

By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.

Related Controls

- SI-12
- TR-1

Applicability

These standards apply to all users of TAMU-CC information and information technology resources regardless of affiliation, and irrespective of whether these resources are accessed from on-campus or off-campus locations, in both centralized and decentralized (distributed) IT environments, owned or managed by the University.

This standard applies to all University data, and are to be followed by Users, Owner, or Custodians, who capture data and manage administrative information systems using university assets

TAMUS Control (DM-1)

Implementation

TAMU-CC shall reduce, and eliminate where possible, the collection and/or use of sensitive personal information [Texas Business and Commerce Code 521.002] in information resources under the control of the University.

Transparency (TR) - 1 control

TR-1 Privacy Notice

Description

Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices.

The organization may provide general public notice through a variety of means, as required by law or policy, including

i. System of Records Notices (SORNs),
ii. Privacy Impact Assessments (PIAs), or
iii. in a website privacy policy.

As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization’s public notices, in consultation with legal counsel and relevant program managers.

The public notice requirement in this Control is satisfied by an organization’s compliance with the public notice provisions of the Privacy Act, the E-Government Act’s PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).

Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel.

Applicability

These standards apply to all users of TAMU-CC information and information technology resources regardless of affiliation, and irrespective of whether these resources are accessed from on-campus or off-campus locations, in both centralized and decentralized (distributed) IT environments, owned or managed by the University.

This standard applies to all University data, and are to be followed by Users, Owner, or Custodians, who capture data and manage administrative information systems using university assets

TAMUS Control (TR-1)

Implementation

TAMU-CC shall publish a privacy notice on websites owned by the University which contains, at a minimum, the content contained on The Texas A&M University System's website.

Acronyms and Abbreviations

- **A&M System**: The Texas A&M University System
- **APT**: Advanced Persistent Threat
- **CAB**: Change Advisory Board
- **CEO**: Chief Executive Officer
- **CIO**: Chief Information Officer
- **CIS**: Center for Internet Security
- **CISPO**: Chief Information Security and Privacy Officer
- **CNSS**: Committee on National Security Systems
- **CPO**: Chief Privacy Officer
- **CVE**: Common Vulnerabilities and Exposures
- **CVSS**: Common Vulnerability Scoring System
- **CWE**: Common Weakness Enumeration
- **DIR**: Texas Department of Information Resources
- **Division of IT**: Division of Information Technology
- **DoD**: Department of Defense
- **DoIT**: Division of Information Technology
- **DMZ**: Demilitarized Zone
- **DNS**: Domain Name System
- **DNSSEC**: Domain Name System Security Extensions
- **FIPS**: Federal Information Processing Standard
- **FISMA**: Federal Information Security Modernization Act
- **FTP**: File Transfer Protocol
- **GMT**: Greenwich Mean Time
- **HTTP**: Hyper Text Transfer Protocol
- **HTTPS**: Hyper Text Transfer Protocol Secure
- **IP**: Internet Protocol

- **IRC**: Internet Relay Chat
- **ISE**: Information Sharing Environment
- **IT**: Information Technology
- **LAN**: Local-Area Network
- **MFA**: Multi-factor Authentication
- **MS**: Microsoft
- **MS RCP or MSRCP**: Microsoft Remote Procedural Call
- **NetBIOS**: Network Basic Input/Output System
- **NAT**: Network Address Translation
- **NIST**: National Institute of Standards and Technology
- **NSA**: National Security Agency
- **NTP**: Network Time Protocol
- **NVD**: National Vulnerability Database
- **OIS**: Office of Information Security
- **OVAL**: Open Vulnerability Assessment Language
- **OMB**: Office of Management and Budget
- **PATS**: Permitted Authorized Time Sources
- **PIA**: Privacy Impact Assessment
- **PII**: Personally Identifiable Information
- **POP or PoP**: Point of Presence
- **REN-ISAC**: Research Education Networking Information Sharing & Analysis Center
- **SAOP**: Senior Agency Official for Privacy
- **Secure FTP**: Secure File Transfer Protocol
- **SCAP**: Security Content Automation Protocol
- **SFTP**: Secure File Transfer Protocol
- **SIEM**: Security Information and Event Managements
- **SMB**: Server Message Block
- **SMTP**: Simple Mail Transfer Protocol

- **SORN**: System of Records Notice
- **SPECTRIM**: Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management
- **SSID**: Service Set Identifiers
- **SSL**: Secure Sockets Layer
- **System**: The Texas A&M University System
- **TAC**: Texas Administrative Code
- **TAMU**: Texas A&M University
- **TAMU-CC**: Texas A&M University-Corpus Christi
- **TAMU System**: The Texas A&M University System
- **TAMUS**: The Texas A&M University System
- **TCP**: Transmission Control Protocol
- **Texas A&M University System**: The Texas A&M University System
- **Texas A&M System**: The Texas A&M University System
- **Texas DIR**: Texas Department of Information Resources
- **TFTP**: Trivial File Transfer Protocol
- **TGC**: Texas Government Code
- **TLS**: Transport Layer Security
- **UDP**: User Data Protocol
- **University**: Texas A&M University-Corpus Christi
- **US-CERT**: United States Computer Emergency Readiness Team
- **US PATRIOT Act**: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
- **USB**: Universal Serial Bus
- **USGCB**: United States Government Configuration Baseline
- **UTC**: University Technology Council
  - or UTC: Coordinated Universal Time
- **VoIP**: Voice Over Internet Protocol

- **VPN**: Virtual Private Network
- **WAN**: Wide-Area Network

Revision History

Last Updated: June 29, 2023

Previous Versions:

- May 31, 2022
- March 25, 2021
- September 16, 2019