Office of Information Technology

THE TEXAS A&M UNIVERSITY SYSTEM

Security Controls Catalog

Approved 10/02/2023

The System Offices Security Controls Catalog establishes the minimum information security requirements for the Texas A&M University System Offices.

This catalog defines controls that have been designated as mandatory by the Texas Department of Information Resources (DIR) and The Texas A&M University System (TAMUS). They are based on the current version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

These controls were developed to align with the DIR Security Control Standards Catalog as required by TAC §202.76, Security Control Standards Catalog, and TAMUS Policy 29.01.03, Information Security.

Each control group is organized under its two-letter group identification code and title and adopts the numbering format of the DIR Security Control Standards Catalog.

Table of Contents

Publication

TAC §202.76(a) requires publication of mandatory controls on the department's website.

Exceptions

Information Resource Owners are responsible for ensuring that the protection measures in the Security Controls Catalog are implemented. Information resource owners may request to exclude certain protection measures mandated by a control in favor of an alternate mitigation based on risk management considerations and business functions.

Any exceptions to the information security controls in this catalog must be approved and documented. Contact the System Offices Information Security Officer (ISO) to request an exception to a security control. Once processed by the System Offices ISO, an opinion for approval or denial will be returned to the requestor.

Definitions

Terms that are used frequently in these standards. Additional definitions can be found in:

- TAC §202.1, Applicable Terms and Technologies for Information Security Standards
- Texas A&M University System Data Classification Standard
- Glossary | CSRC (nist.gov)

Information Resource / Information System

IT hardware and software systems. This includes:

- data,
- equipment, facilities, and software, that create, process, store, retrieve, display, or transmit data, and
- any computer-related activities involving any device capable of receiving, storing, managing, or transmitting data.
- Examples include, mainframes, servers, network infrastructure, desktop and laptop computers, IP phones, printers, web applications and cloud services.

Information Resources Manager (IRM)

The executive responsible for Information Resources across the institution as defined in Chapter 2054, Subchapter D, Texas Government Code. This is the Texas A&M University System Offices Chief Information Officer.

Information Resource Owner

- The person who is legally or operationally responsible and accountable for the data and/or business function that is supported by an information resource.
- The Owner determines controls and access to information resources supporting that business function.
- Typically, this is a department head and may be the person responsible for the procurement, development, operation, and maintenance of an information resource.

Information Resource Custodian

An individual, department, institution, or third-party service provider responsible for supporting and implementing owner-defined controls to information resources. Custodians include information technology units, staff, vendors, and any third-party acting as an agent of or otherwise on behalf of the Office of Information Technology.

High Impact Information / Information Resources

Information and information resources that are essential to the mission and operations of the Texas A&M University System or the System Offices.

Loss or disruption to the confidentiality, integrity, or availability of a High Impact Information Resource would result in a **severe or catastrophic adverse effect** on organization operations, assets, or individuals. Such an event could:

a. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
b. result in major damage to organizational assets;
c. result in major financial loss; or
d. result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

This term equates to HIGH impact in the Federal Standards for Security Categorization of Federal Information and Information Systems, FIPS 199.

Moderate Impact Information / Information Resources

Information and information resources whose loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. Such an event could:

a. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
b. result in significant damage to organizational assets;
c. result in significant financial loss; or
d. result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

Low Impact Information / Information Resources

Information and information resources whose loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. Such an event could:

a. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
b. result in minor damage to organizational assets;
c. result in minor financial loss; or
d. result in minor harm to individuals.

Access Control

AC-1, Access Control Policy and Procedures

Access Control Policy

The Texas A&M University System Offices recognizes that access control policies and procedures are vital to reducing information security risks.

Purpose

The Access Control Policy and associated controls describe the requirements for providing access to System Offices Information Resources. Requirements are defined for managing accounts and implementing access controls, separation of duties and least privilege.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

The Access Control Policy and associated controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for ensuring that access controls are implemented for the information resources under their control.
b. The System Offices ISO (SO ISO) or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

AC-2, Account Management

a. Each user of System Offices-owned information resources must be assigned a uniquely identifiable account.
b. An approval process is required before granting access authorization for an information resource. The approval process must:
    1. positively establish the identity of a user and determine the appropriate user role(s) before access is granted; and
    2. document the account holder's acknowledgement that they have read and agree to the Acceptable Use Standards, Rules of Behavior and to their responsibilities as a user of System Offices information resources.
c. Before an account is enabled:
    1. the account holder's supervisor or sponsor must approve the account by signing the Statement of Responsibility (SOR) form; and
    2. the new user must sign the SOR and Acceptable Use Standards.
d. Accounts must be reviewed periodically. Logon IDs that have not been accessed within a reasonable period (as established by risk management decisions) from the date of creation will be disabled.

Types of Information System Accounts

Information system account types include: System Offices employee Users, Sponsored Guest Users, Emeritus Users, Administrator Users (for Workstation/Server/Domain/Application), Local Administrators, and Service Accounts.

a. **System Offices Employee Users** are budgeted, wage, graduate assistant, student worker, working retiree, retiree emeritus, and other employees administratively located (ADLOC) in Parts 01, 26 and 27 of the Texas A&M University System (TAMUS System Offices).
    1. These accounts are requested by the hiring authority for a new employee by completing the Statement of Responsibility (SOR) form. Users must sign the SOR before receiving an account. By signing, the user acknowledges their understanding and agreement to follow the Acceptable Use Standards, rules of behavior and their responsibilities as a user of System Offices information resources.
    2. These accounts are disabled upon termination of employment or other circumstances deemed appropriate by the supervisor, human resources, the System Offices Information Security Officer (SO ISO), or their designee. See control PS-4.
    3. These accounts are disabled after an appropriate duration of inactivity (typically 6 months).

b. **Sponsored Guest Users** are System Offices affiliates, contractors, vendors, visiting scholars, and other users that require workstation access or access to specific information resources.
    1. These accounts are requested by a System Offices employee authorized to sponsor the user. Accounts are requested by completing the SOR form for third parties.
    2. These accounts are provisioned by the Information Resource Custodian once approved by the sponsor's program manager/department head and the SOR for third parties is signed.
    3. These accounts are valid for up to one year and are automatically disabled on the scheduled expiration date. The account sponsor can renew the account by submitting an updated SOR for third parties.
    4. These accounts are disabled upon termination of employment or other circumstances deemed appropriate by the supervisor, human resources, SO ISO or their designee. See control PS-4.
    5. These accounts are disabled after an appropriate duration of inactivity (typically 90 days).
c. **Emeritus Users** are faculty, staff and regents granted the “Emeritus” designation upon retirement by the Texas A&M University System Board of Regents.
    1. These users may retain access to System Offices email.
d. **Administrator Users** are Information Technology staff with a valid business need for privileged access to an information resource such as a workstation, server, or an enterprise application.
    1. These accounts are requested by the user, their program manager, department head, or higher authority.
    2. These accounts are approved by the user's program manager/department head and the System Offices Chief Information Officer’s (SO CIO) designee for the information resource after review of the request's scope and justification.
e. **Local Administrator Accounts** are non-domain accounts with privileged access to an information resource such as an individual workstation, server, or enterprise application.
    1. The operating system local administrator account must be disabled and have a randomly generated password that is regularly updated through an automated process.
    2. Local administrator accounts must be approved by the Information Resource Owner and the SO CIO’s designee for the information resource.
    3. Local administrator accounts must be documented as a security control exception.
f. **Service Accounts** are managed domain accounts for the specific purpose of machine-to-machine automated interaction.
    1. These accounts are requested by the owner/custodian for the information resource where the account will be implemented and approved by the SO CIO’s designee after review of the request's scope and justification.

2. Where feasible, Microsoft Managed Service Accounts (MSAs) should be used. The domain handles the password, changes it on a regular basis and a human never knows the password.
3. For information resources requiring a service account that do not support MSAs:
    i. These accounts are valid indefinitely and require a long, complex password that must be updated on a scheduled basis not to exceed 365 days, or when a user with knowledge of the account password is no longer approved for access.
    ii. These accounts are de-provisioned by the resource manager when they are no longer required.

Conditions for security group and distribution group membership

Membership in security and distribution groups will be requested by the Information Resource Owner or their designee and submitted to IT.

Account monitoring, review, and notifications

Information Resource Owners or their designees, are responsible for reviewing group membership on a regular basis (not to exceed every 12 months) to ensure that membership is limited to users with a valid business purpose.

AC-2(7), Privileged User Accounts

Information Resource Owners or their designees are responsible for:

a. Establishing and administering privileged (also known as administrative or special access) accounts.
b. Monitoring the assignment of roles or attributes that provide elevated privileges.
c. Monitoring changes to roles or attributes that provide elevated privileges.
d. Ensuring that elevated access is revoked when no longer needed.
e. Ensuring that users with privileged accounts are aware of the extraordinary responsibilities associated with the use of these accounts.

AC-3, Access Enforcement

a. Information Resource Custodians are responsible for managing access to System Offices information resources.
b. Each user of System Offices information resources will be assigned a unique identifier.
c. Identification and authentication are required before a user is able access and perform an action on an information resource.

Note: Control AC-14 defines permitted actions without identification or authentication.

AC-3(7), Role-based Access Control

a. Where feasible, information resources will implement role-based access control (e.g. employee users, guest users, etc.).
b. Access to data and functions will be based on job function following the principle of least privilege (defined in control AC-06).

AC-5, Separation of Duties

The principle of separation of duties reduces risk by preventing errors and/or abuse. Separation of duties is required for High Impact Information Resources.

a. Information Resource Owners or their designees are responsible for ensuring that controls are implemented to support the principle of separation of duties for information resources under their control.
b. Information Resource Owners or their designees must maintain a list of individuals who have administrative or special access accounts for resources they control. The list must be reviewed by the Information Resource Owner or their designee on a regular basis.
c. Requirements for High Impact Information Resources:
    1. Separate development, test, and production environments must be implemented.
    2. Where feasible, development and test systems should have appropriate forms of isolation from production systems. For example, development, test, and production systems may each use separate virtual servers that are isolated from each other.

3. Source code must be reviewed and approved by an authorized individual or group designated by the Information Resource Owner before release into a production environment.
4. There must be appropriate separation between members of the development team and those who are allowed to deploy code to the production environment.

d. Financial systems developed by the System Offices must ensure that a person who enters a financial transaction is not the same person who authorized payment to be made from that transaction.
e. Source code developed within the System Offices for High and Moderate Impact Information Resources must be committed to a code repository approved by the Information Resource Owner or their designee.
f. Individuals who use administrative or special access accounts must use the account most appropriate for the work being performed (e.g., user account vs. administrator account). See control AC-6.
g. The password for a shared administrator or special access account must be changed if:
    1. an individual knowing the password leaves employment; or
    2. job duties change and the individual no longer performs functions requiring such access; or
    3. a contractor or vendor with such access leaves or completes their work.
h. Development and testing tools must be removed or disabled on production systems when they are not required.

AC-6, Least Privilege

The principle of least privilege is employed for System Offices information systems. Users (or processes acting on behalf of users) must only have the access necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

a. Accounts must be created with a baseline appropriate for the category of account. (For example, System Offices Users receive a minimum level of access to information resources approved for all employees).
b. Information Resource Custodians are responsible for ensuring that access is given to the minimum degree necessary for users to accomplish assigned tasks.
c. Administrator and special access accounts are only authorized to perform limited privileged access tasks, such as system maintenance and administration.
d. Sensitive tasks such as account management must be restricted to members of specific privileged security groups created for that purpose.
e. Information Resource Owners or their designees are responsible for ensuring that users with administrative accounts are aware of the extraordinary responsibilities associated with the use of privileged accounts.
f. Privileges should be escalated only when necessary to accomplish assigned tasks.

AC-7, Unsuccessful Logon Attempts

a. As technology permits, information resources should enforce account lockouts after 10 failed attempts at minimum.
b. Accounts locked due to multiple incorrect logon attempts should stay locked for a minimum of 15 minutes. Information Resource Owners can choose to require that an administrator reset accounts when they are locked.

AC-8, System Use Notification

a. The system use notification message must be displayed to users before they are granted access to System Offices information systems where feasible.

System Offices System Notification Message:

TAMUS Disclaimer

This computer system and all data herein are official State of Texas resources and as such are available only for authorized purposes by authorized users. Use for any other purpose may result in administrative/disciplinary actions or criminal prosecution against the user. Usage is subject to monitoring and security testing. The user should have no expectation of privacy except as otherwise provided by applicable privacy laws.

AC-14, Permitted Actions without Identification or Authentication

a. Publicly accessible information resources such as public websites, information kiosks and other situations where risk analysis demonstrates no need for individual accountability are exempt from the requirement to identify specific users specified in control AC-3.
b. Exceptions must be approved by the System Offices Information Security Officer or their designee and documented.

AC-17, Remote Access

a. All forms of remote access must have appropriate safeguards to protect the confidentiality, integrity, and availability of the information resource. Example safeguards include encrypted communication channels, and multi-factor authentication.
b. Remote access to an information resource must be approved by the System Offices Chief Information Officer's (SO CIO) designee and the System Offices Information Security Officer (SO ISO) before access is made available.
c. Information Resource Owners or their designees are responsible for documenting usage restrictions, configuration/connection requirements and implementation guidance if remote access to systems under their control is allowed. At a minimum:
    1. Remote access to System Offices-owned information resources must be conducted using a System Offices controlled, encrypted point-to-point tunnel. Examples include the System Offices Virtual Private Network (VPN), SSH, Microsoft Remote Desktop Protocol (RDP) over TLS, TN3270 over TLS and HTTPS over TLS.
    2. Connections must be encrypted following controls SC-12 and SC-13.
    3. RDP must be configured to require appropriate network encryption such as TLS.
    4. RDP and SSH connections must initiate within the System Office's protected network or through a secure gateway. Public access for these services is not allowed.

AC-18, Wireless Access

a. Wireless Network access at System Offices locations is provided by the Texas A&M University Division of Information Technology. Texas A&M IT Policy, AC-18 Wireless Access applies to this network.
b. Unauthorized access points and network attached wireless devices are not allowed on the System Offices network.

AC-19, Access Control for Mobile Devices

a. System Offices-owned mobile devices must require a passcode that is 4 digits or longer or require biometric authentication such as a fingerprint or face scan.
b. System Offices-owned mobile devices must be encrypted, kept up to date/patched, and have a firewall enabled.
c. Critical or Confidential data must not be transmitted through a wireless connection to, or from a mobile computing device without appropriate encryption such as TLS.
d. Unattended mobile devices must be kept physically secure using a method that is appropriate for the associated risk.
e. System Offices-owned mobile devices must be managed by a mobile device management (MDM) system.

Note: This control applies to all System Offices-owned mobile devices. Control AC-20 addresses mobile devices that are not organization-controlled.

AC-20, Use of External Systems

a. Before use, external information resources that access, process, store or transmit data controlled by the System Offices, must be approved by the System Offices Chief Information Officer's (SO CIO) designee for the information resource and the System Offices Information Security Officer (SO ISO) or their designee. See controls SA-4 and SA-9.
b. Personally owned devices that connect to the System Offices email system must be kept up to date/patched, and use a password, passcode, or another form of authentication to prevent unauthorized access to the device.

AC-22, Publicly Accessible Content

a. Information Resource Owners who have publicly accessible information resources under their control are responsible for:
    1. designating Information Resource Custodians who are authorized to post information onto the publicly accessible information resource;
    2. ensuring that training is provided to ensure that publicly accessible information resources do not expose nonpublic information;
    3. ensuring that content is reviewed before it is published to the publicly accessible information resource to confirm that it does not contain nonpublic information; and

4. ensuring that content is reviewed periodically after it is published to the publicly accessible information resource to confirm that it does not contain nonpublic information and remove such information if discovered.

b. Mandatory security awareness training is assigned to all System Offices personnel annually. It provides guidance on protecting nonpublic information. Additional training on preventing the disclosure of nonpublic information for specific roles and applications may be provided as needed.

Awareness and Training

AT-1, Awareness and Training Policy and Procedures

Security Awareness Training Policy

Purpose
The Texas A&M University System Offices recognizes that security awareness training policies and procedures are vital to reducing information security risks.

The Security Awareness Training Policy and associated controls document the requirements for training users to understand their responsibilities under State law and System policy, and their role in protecting the System Offices Information Resources by reducing information security risks.

Scope and Roles
The intended audience includes the System Offices Information Security Officer (SO ISO) and all users of System Offices Information Resources.

Compliance
The Security Awareness Training Policy and associated controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76, §202.74, Texas Government Code §2054.519, §2054.5191, §2054.5192, and Texas A&M University System Policy 29.01.03, Information Security.

Implementation
The SO ISO or their designee is responsible for:

a. documenting and disseminating procedures that address the Awareness and Training family of controls; and
b. ensuring that this policy and supporting procedures are periodically reviewed and updated.

AT-2, Literacy Training and Awareness

a. The Texas A&M University System Offices administers security and privacy awareness training in compliance with the requirements of TAC §2054.5191–.5192 and System Policy 29.01.03 for all users including mangers, senior executives, contractors, and other sponsored guest users.
b. Training will be provided through the TAMUS-approved approved training system and recorded.
    1. All users of System Offices-owned information resources must complete a TAMUS approved Information Security Awareness course immediately upon hire and every year after.
    2. If the training material changes substantially, the System Offices Information Security Officer (SO ISO) may choose to have all users, or a specific segment of users retake the training out-of-cycle.
c. The SO ISO may use other communications channels (such as email and awareness campaigns such as National Cyber Security Awareness Month) to inform users of information security awareness topics.
d. Training and awareness content will be updated periodically to incorporate lessons learned from internal or external security incidents.

AT-3, Role-based Training

a. Additional role-based security and privacy training may be assigned based on factors such as information resource risk or scope of assigned duties. The System Offices Information Security Officer, Information Resource Owners and managers may assign additional training before authorizing access to systems or on an as-needed basis.
b. Role-based training will be updated periodically to incorporate lessons learned from contingency plan testing, internal or external security incidents. See controls CP-4, IR-2.

AT-4, Training Records

a. The Texas A&M University System training management system is the system of record for information security awareness training.

b. Training records for the required security and privacy awareness training are maintained in accordance with the Texas A&M University System records retention schedule.
c. Documentation for specialized training may be maintained by individual supervisors.

Audit and Accountability

AU-1, Audit and Accountability Policy and Procedures

Audit and Accountability Policy

The Texas A&M University System Offices recognizes that information system auditing policies and procedures are vital to reducing information security risks.

Purpose

The Audit and Accountability Policy and associated controls document the requirements for ensuring there are adequate event and transaction logs to account for, respond to, and minimize the impact of incidents that can impact System Offices Information Resources.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

Audit and Accountability controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

The SO ISO or their designee is responsible for:

a. documenting and disseminating procedures that address the Audit and Accountability family of controls for the information resources under their control; and
b. ensuring that this policy and supporting procedures are periodically reviewed and updated.

AU-2, Event Logging

a. Information resources must keep security-related event logs that establish individual accountability for actions that can potentially threaten the confidentiality, integrity, or availability of the information resource.
b. Based on periodic risk assessments, Information Resource Custodians, and the System Offices Information Security Officer (SO ISO) are responsible for ensuring that information systems log a sufficiently complete history of transactions to support an after-the-fact investigation by logging and tracing the activities of individuals through the system.
c. The SO ISO or their designee is responsible for reviewing and updating the event types selected for logging periodically.
d. The types of events that require logging include:
    1. Any action that can potentially cause access to, creation of, modification of, or affect the release of Confidential or Controlled information.
    2. Any significant event that is relevant to the security of systems, including password changes, failed logons, failed access events, security or privacy attribute changes, administrative privilege usage, all changes to automated security or access rules.
    3. Updates to High Impact Information Resources.
e. Information Resource Custodians and the A&M System Cybersecurity must coordinate event logging functions with each other.

AU-3, Content of Audit Records

Where feasible, Information Resource Custodians should use the Center for Internet Security (CIS) Benchmarks Level I standards to configure event logging. Audit records contain information that establishes the following:

a. The type of event that occurred.
b. When the event occurred.
c. The software or hardware component of the information resource where the event occurred.
d. The source of the event (e.g. network address).
e. The outcome (success or failure) of the event.
f. Identity of any individuals, subjects, or objects associated with the event.

AU-4, Audit Log Storage Capacity

Information Resource Custodians are responsible for ensuring that sufficient audit record storage is available.

a. Sufficient storage must be allocated to meet the data retention requirements for each information system.
b. Information Resource Custodians must configure auditing to reduce the likelihood of exceeding audit storage capacity.

AU-5, Response to Audit Logging Process Failures

Logging failures include an application or operating system failing to log events, a failure to send events to the central logging system or a failure of the central logging system itself.

a. Information Resource Owners or their designees, including the owner of the centralized logging system, are responsible for:
    1. specifying appropriate monitoring for logging failures for the systems under their authority;
    2. defining audit alert thresholds for the systems under their authority; and
    3. designating appropriate contacts to receive alerts for the systems under their authority.
b. Information Resource Custodians are responsible for configuring information systems to:
    1. automatically send alerts in the event of an audit logging failure;
    2. automatically send alerts for low storage capacity for audit logs; and
    3. overwrite the oldest audit logs to reduce the chance of an incident in the absence of auditing and accountability.

AU-6, Audit Record Review, Analysis, and Reporting

a. Information Resource Custodians are responsible for:

1. routinely reviewing information system audit logs for indications of security incidents and other unusual or suspicious activity at a frequency appropriate for the level of risk;
2. reporting security incidents, and other unusual or suspicious activity to the Information Resource Owner and the System Office Information Security Officer following the processes defined in Control Standards IR-1 and IR-6; and
3. updating the level of log review and reporting when there is a change in risk for an information system.

AU-8, Time Stamps

a. Information Resource Custodians are responsible for:
    1. configuring information resources to use internal system clocks to generate time stamps, including date and time, for audit logs;
    2. configuring information resources to record time stamps for audit logs that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) within an acceptable degree of accuracy; and
    3. configuring information resources to synchronize clocks with a Stratum-1 time source where feasible.

AU-9, Protection of Audit Information

a. Information Resource Custodians are responsible for:
    1. ensuring that audit logs and related tools are protected so only authorized individuals and systems can access them;
    2. configuring information resources to protect audit information and audit tools from unauthorized access, modification, or deletion; and
    3. configuring information resources to send alerts to appropriate personnel upon detection of unauthorized access, modification, or deletion of audit information.

AU-11, Audit Record Retention

a. Information Resource Custodians are responsible for:

1. ensuring that sufficient audit logs are retained to support for after-the-fact investigations of information security incidents and to meet record retention requirements; and
2. maintaining audit logs associated with known incidents, including those used for legal action, until the incident is closed.

Related Requirements

Texas A&M University System Records Retention Schedule

Texas Government Code §441.187 Destruction of State Records

Texas Administrative Code §6.95 Final Disposition of Electronic State Records

AU-12, Audit Record Generation

a. Information Resource Custodians are responsible for ensuring that information systems generate audit logs following the list of event types defined in control AU-2 with the content defined in control AU-3 on the following types of information systems:
    1. High Impact Information Resources, including applications;
    2. servers (including application servers, database servers, file servers, security appliances and web servers);
    3. network components (including switches, routers, wireless access points); and
    4. desktop and laptop computers.
b. Information Resource Custodians will work with the System Offices Information Security Officer or their designee to determine which systems and event types to send to the central logging system.

Assessment, Authorization and Monitoring

CA-1, Assessment, Authorization and Monitoring Policy and Procedures

Assessment, Authorization, and Monitoring Policy

The Texas A&M University System Offices recognizes that information security assessment, authorization, and continuous monitoring policies and procedures are vital to reducing information security risks.

Purpose

Assessments and monitoring ensure that information security controls are implemented correctly, working as intended and result in meeting the security requirements for each information resource.

Authorization to operate information resources must be controlled to ensure that residual risks are reviewed and accepted and to ensure that authorized resources satisfy business needs and comply with security, privacy, and accessibility laws and policies.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

Assessment, authorization, and monitoring controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the Assessment, Authorization and Monitoring family of controls for the information resources under their control.
b. The SO ISO or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

CA-2, Control Assessments

Texas Administrative Code (TAC) §202.76(c) requires an assessment of the System Offices information security program for compliance with TAC §202 including the security controls required by The Texas Department of Information Resources (DIR).

a. The System Offices Information Security Officer (SO ISO) or their designee is responsible for developing a control assessment plan that describes the scope of the assessment including:
    1. controls under assessment;
    2. assessment procedures used to determine the effectiveness of each security control; and
    3. assessment environment, team, roles, and responsibilities.
b. The security controls assessment will:
    1. review the System Offices security controls and the environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, meeting security requirements and producing the desired outcome;
    2. be performed by individual(s) independent of the SO ISO; and
    3. be performed at least every other year based on risk management decisions.
c. Assessment results will be reported to the Chancellor, the SCIO, SO CIO, and other executive leadership.

Note: this control is distinct from the information security risk assessments described in control RA-3, Risk Assessment.

CA-3, System Interconnections

The designated IT department authorizes all dedicated connections from the organization's information resources to external information systems. Generally, connections are in scope if

they are dedicated and (semi)-permanent. This control does not apply to user-controlled, transitory connections (such as email, or website browsing).

a. Interconnection security agreements for non-publicly accessible information must be established with all outside information providers/consumers.
b. Interconnections must be approved by the System Offices Information Security Officer (SO ISO) or their designee and the System Offices Chief Information Officer's (SO CIO) designee for the information resource.
c. Each exchange agreement must document:
    1. the purpose of the connection;
    2. the nature of the information communicated including the TAMUS data classification, and FIPS 199 impact levels;
    3. interface characteristics including host names or IP addresses, data transfer method, ports, and protocols;
    4. security and privacy requirements; and
    5. data transfer frequency.
d. The SO ISO is responsible for ensuring that interconnection security agreements are reviewed periodically.

CA-5, Plan of Action and Milestones

a. Information Resource Owners or their designees are responsible for developing actionable plans to respond to risks identified through information security assessments.
b. Risk Assessment Action Plans will document the steps to fix deficiencies or compensating controls that will be implemented to mitigate each risk, and any proposed security control exceptions that will be requested as part of the mitigation.
c. Action plans must be submitted to the System Offices Information Security Officer (SO ISO).

CA-6, Security Authorization

a. The System Offices Chief Information Officer (SO CIO) has delegated authorization to operate System Offices information resources to Information Resource Owners and the leadership of each IT department.
    1. Information Resource Owners or their designees are responsible for ensuring that authorized resources satisfy business needs.

2. The relevant IT department will ensure that authorized resources comply with security, privacy, and accessibility laws and policies.

b. An Information Resource Owner must be identified for each information system. Information Resource Owners are accountable for security and privacy risks associated with the operation and use of the information systems under their authority.
c. The Information Resource Owner and the IT department are responsible for authorizing information resources before they begin operation.

CA-7, Continuous Monitoring

a. The System Offices Information Security Officer (SO ISO) or their designee must develop and implement a Continuous Monitoring Plan that includes:
    1. a list of the information resource metrics to be monitored;
    2. a methodology for monitoring and assessing the effectiveness of security controls;
    3. ongoing security status monitoring of defined metrics;
    4. correlation and analysis of security related information generated by assessments and monitoring;
    5. response actions to address results of the analysis of control assessment and monitoring information; and
    6. reporting the information security status of the System Offices to the System Offices Chief Information Officer.

CA-7(4), Risk Monitoring

a. The following risk monitoring items should be included in the continuous monitoring plan:
    1. monitoring to determine the ongoing effectiveness of the implemented risk response measures;
    2. compliance monitoring to verify that required risk response measures are implemented; and
    3. change monitoring identify changes to organizational systems and environments of operation that may affect security.

CA-8, Penetration Testing

a. Vulnerability tests and penetration tests must be conducted on a recurring basis on Internet websites and mobile applications that are exposed to the public internet that process any sensitive personal information, or confidential information as required by Texas Government Code §2054.516(a)(2).
b. Vulnerability tests should be conducted on High Impact Information Resources on a recurring basis.
c. Any vulnerabilities identified must be addressed in a time period determined by the System Offices Information Security Officer (SO ISO) in coordination with Information System Owners.
d. Results from vulnerability and penetration tests must be reported to the System Offices ISO periodically.

CA-9, Internal System Connections

Information Resource Owners are responsible for:

a. authorizing internal interconnections (internal connections for a class of components with common characteristics and/or configurations may be authorized as a group);
b. ensuring internal connections are documented including:
    1. Purpose of the connection.
    2. Nature of the information communicated including the TAMUS data classification, and the Federal Information Processing Standards (FIPS) 199 impact levels.
    3. Interface characteristics including host names or IP addresses, data transfer method, ports, and protocols.
    4. Security requirements and other relevant details about how the information is protected (e.g. authentication, encryption, and firewall rules).
    5. Data transfer frequency.
c. ensuring that internal interconnections are reviewed periodically to update documentation and terminate connections that are not in use.

Configuration Management

CM-1, Configuration Management Policy and Procedures

Configuration Management Policy

The Texas A&M University System Offices recognizes that configuration management policies and procedures are vital to reducing information security risks.

Purpose

The Configuration Management Policy and associated controls describe the requirements for managing risks associated with configuring new information systems, controlling changes to information systems, configuration, and security settings. Requirements are also defined for reducing information security risk by implementing least functionality, an information system inventory, and software use restrictions.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes Information Resource Owners and Custodians.

Compliance

Configuration Management controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the Configuration Management family of controls for the information resources under their control.

b. The System Offices Information Security Officer (SO ISO) or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

CM-2, Baseline Configuration

Common security configurations must be developed to provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources.

a. Information Resource Custodians are responsible for developing, documenting, and maintaining a current baseline configuration for High Impact information resources under their control.
    1. Based on risk, a baseline security configuration should be selected from industry best-practice baselines such as the Department of Defense Security Technical Implementation Guides (STIG), the Center for Internet Security Benchmarks or vendor-supplied baselines.
    2. A baseline should be developed if a government or vendor baseline does not exist. The baseline should ensure that the principles of least privilege and least functionality are followed. Non-essential capabilities, ports, protocols and/or services must be disabled or restricted where feasible.
    3. Unnecessary software including services, and drivers should be removed.
    4. Default accounts should be removed or disabled, or the password must be changed before placing a resource on the network where feasible.
    5. Recommended security features included in vendor-supplied systems must be enabled including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections.
    6. Up-to-date security patches must be applied before an Information Resource is deployed.
b. Baseline configurations must be reviewed and updated as appropriate when there are significant changes to a High Impact information resource.

CM-3, Configuration Change Control

a. Information Resource Owners or their designees are responsible for determining and documenting the types of changes that are configuration-controlled and the change control process for the information systems under their control. The change control process should address:

1. how changes are identified, classified, prioritized, and requested;
2. identification and deployment for emergency changes;
3. assessing potential impacts from changes;
4. authorizing changes and exceptions; and
5. implementing changes and planning for back-outs.

b. Configuration-controlled changes must:
   1. be documented, including approval decisions, a date and timeframe for the change and the result after the change is made;
   2. be reviewed to consider their potential impact to users, stability of the system and dependent resources, and impact to security, and privacy then approved or disapproved; and
   3. have appropriate communications and coordination with anyone who will be impacted.

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

Information Resource Owners or their designee are responsible for determining the types of changes that are configuration-controlled as specified in control CM-3.

a. Configuration-controlled changes to Moderate Impact Information Resources should be tested, validated, and documented before finalizing their implementation.
b. Configuration-controlled changes to High Impact Information Resources **must** be tested, validated, and documented before finalizing their implementation.

CM-4, Impact Analysis

a. Information Resource Custodians are responsible for ensuring that changes are analyzed to determine if there are potential security or privacy impacts before implementation.

CM-5, Access Restrictions for Change

a. Information Resource Owners or their designees are responsible for designating individuals who are authorized to implement changes to information resources under their control.
b. Where feasible, access restrictions must be implemented so changes can only be made by authorized individuals.
c. Access restrictions must be documented.

CM-6, Configuration Settings

a. Information Resource Custodians are responsible for:
    1. establishing and documenting mandatory configuration settings for information resources;
    2. configuring security settings in the most restrictive mode consistent with operational requirements;
    3. documenting configuration settings (i.e., in the information resource, or in a checklist or configuration file);
    4. enforcing the configuration settings in all components in the information resource; and
    5. monitoring and controlling changes to the configuration settings in accordance with organizational policies and procedures.

CM-7, Least Functionality

a. Information Resource Custodians must ensure that information resources under their control are configured to provide only the essential capabilities required for business needs.

CM-8, Information System Component Inventory

a. Information Resource Custodians must maintain an inventory of the components for High Impact Information Resources.

Note: Additional inventory requirements are documented in control PM-5. Component inventories are included in the system security plans documented in control PL-2, and the annual report on the information security program documented in control PL-1.

CM-10, Software Usage Restrictions

a. Information Resource Owners or their designees must ensure that:
    1. software is used in accordance with applicable software license(s) as required by System Policy 29.01.02 and the U.S. Copyright Act; and
    2. tracking software use, to ensure compliance with contract agreements and copyright laws where feasible.

CM-11, User-Installed Software

a. All software installed on System Offices-owned computer systems must be appropriately licensed.
b. The individual installing or authorizing the installation of software is responsible for being familiar with the terms of the license agreement.
c. Individuals or departments should maintain sufficient documentation to validate that software is appropriately licensed (e.g., End User License Agreements, purchase receipts).
d. Software may not be copied or installed unless specifically allowed by the licensing agreement.
e. Software that can be installed by users without elevated privileges is allowed; users are strongly encouraged to check with Information Technology to learn if there are known security, privacy, compatibility, or licensing issues with new software.

f. Software that requires elevated privileges to install or run must be approved by the System Offices Chief Information Officer's (SO CIO) designee for the information resource.

Contingency Planning

CP-1, Contingency Planning Policy and Procedures

Contingency Planning Policy

The Texas A&M University System Offices recognizes that contingency planning policies and procedures are vital to reducing information security risks.

Purpose

The Contingency Planning Policy and associated controls describe the requirements for written plans to minimize the effects of a disaster, and either maintain or quickly resume mission-critical information technology functions.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes Information Resource Owners and Custodians.

Compliance

Contingency plans for information resources are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Information resource contingency plans are a component of the Office of Information Technology (OIT) Business Continuity Plan.

The OIT Business Continuity Plan is a component of the System Offices Business Continuity Plan which is required by System Policy 34.07.02 and Texas Labor Code §412.054.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the Contingency Planning family of controls for the information resources under their control.
b. The System Offices Information Security Officer (SO ISO) or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated; and
c. Information Resource Owners and the SO ISO or their designees are responsible for reviewing requirements for information resources in the System Offices Business Continuity Plan when the plan is reviewed and updated as part of the safety and security audit conducted every three years as specified by System Policy 34.07.01.

CP-2, Contingency Plan

a. Information Resource Owners or their designees are responsible for developing and maintaining a contingency plan for High Impact Information Resources. The plan for each system will include:
    1. a plan for maintaining essential mission and business functions despite a system disruption, compromise, or failure to the extent feasible;
    2. a Business Impact Analysis including:
        i. an assessment of the impact and magnitude of loss or harm that will result if a major or catastrophic event happens;
        ii. a listing of essential mission and business functions supported by the information resource and any associated contingency requirements.
        iii. recovery time objectives, recovery point objectives, and restoration priorities;
        iv. relevant contact information for organizations or individuals who provide or receive data and support the resource's infrastructure;
        v. a listing of dependent information resources; and
        vi. recovery procedures for High Impact information if cryptographic keys are lost.
    3. a Disaster Recovery Plan as documented in control CP-10; and
    4. steps to coordinate with the A&M System Cybersecurity for handling information security incidents.
b. Contingency plans must be:
    1. reviewed and updated periodically;
    2. distributed to key personnel; and
    3. protected from unauthorized disclosure and modification.

CP-3, Contingency Training

a. The Information Resource Owner or their designee will ensure that training is provided to personnel who have roles and responsibilities related to the Office of Information Technology (OIT) Departmental Business Continuity Plan or component Contingency Plans.
b. Training will be assigned when staff assume a role or responsibility related to a contingency plan or as required by significant changes to a plan.

CP-4, Contingency Plan Testing

a. Backup and recovery procedures documented in Disaster Recovery Plans will be tested periodically.
    1. Annual tests are required for High Impact Information Resources (Texas A&M University System Policy 29.01.03).
b. Lessons learned from testing, training, or actual contingency activities will be documented and incorporated into the Disaster Recovery Plan and training. See control AT-3.
c. Test results will be sent to the System Offices Chief Information Officer for review.
d. Corrective actions from the review of the test report will be sent to Information Resource Custodian(s) for action. Updates to the Disaster Recovery Plan and procedures for backup and recovery will be made if necessary.

CP-6, Alternate Storage Site

a. The System Offices must operate an alternate site that is configured to facilitate the timely and effective recovery and operation of High and Moderate Impact Information Resources.
b. The alternate site must provide appropriate geographical separation so an event would not impact both the primary and alternate site.
c. Alternate sites must provide monitoring, physical and logical security controls that are equivalent to the primary site.

CP-9, Information System Backup

a. High and Moderate Impact Information Resources must be backed up to an alternate site defined in CP-6.
    1. Backup frequency will be consistent with Recovery Point Objectives documented in the Contingency Plan for each information resource (see control CP-2).
    2. Recovery procedures must be documented in the Disaster Recovery Plan for each information resource.
b. The confidentiality, integrity, and availability of backup information must be protected.

CP-9(3), Separate Storage for Critical Information

a. High Impact Information Resources must be protected with a backup strategy that uses immutable backup storage and/or an out-of-band backup process that protects against malicious attacks such as ransomware as required by Texas A&M University Policy 29.01.03.

CP-10, Information System Recovery and Reconstitution

a. Information Resource Owners or their designees are responsible for maintaining a Disaster Recovery Plan (DRP) for each High and Moderate Impact Information Resource. Each DRP will include:
    1. procedures for activating information resources at an alternate site to resume and sustain critical business functions during a contingency;
    2. recovery resources including license keys if applicable;
    3. disaster recovery roles, responsibilities, and assigned individuals with contact information;
    4. step-by-step instructions for a full system restoration without deterioration of security controls; and
    5. process for validating the recovery.

CP-11, Alternate Communications Protocols

a. Alternate communication protocols to support continuity of operations during a contingency must be documented in the Office of Information Technology Business Continuity Plan.

Identification and Authentication

IA-1, Identification and Authentication Policy and Procedures

Identification and Authentication Policy

The Texas A&M University System Offices recognizes that identification and authentication policies and procedures are vital to reducing information security risks.

Purpose

The Identification and Authentication Policy and associated controls describe the requirements for identifying users and protecting access to information resources.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO) and all users of System Offices Information Resources.

Compliance

Identification and Authentication controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

The SO ISO or their designee is responsible for:

1. documenting and disseminating procedures that address the Identification and Authentication family of controls; and

2. ensuring that this policy and supporting procedures are periodically reviewed and updated.

Note: additional identification and authentication requirements are documented in the Access Control (AC) family of controls.

IA-2, Identification and Authentication (Organizational Users)

a. Organizational users must be uniquely identified and authenticated before access is granted to an information resource as specified in control AC-2.
    1. As specified in control AC-14, public websites, information kiosks and other situations where risk analysis demonstrates no need for individual accountability of users are exempt.

IA-2(1), Multi-factor Authentication to Privileged Accounts

a. Multi-factor Authentication (MFA) must be implemented for privileged accounts.

IA-2(2), Multi-factor Authentication to Non-privileged Accounts

a. Multi-factor Authentication (MFA) must be implemented for non-privileged accounts when using remote operating system access (i.e. Remote Desktop, or SSH).
b. MFA is required for access to information resources containing information categorized as Confidential as required by System Policy 29.01.03, and for access to other High and Moderate Impact Information Resources.

IA-4, Identifier Management

a. Information Resource Custodians will manage identifiers for users and devices. A user's access authorization will be appropriately modified or removed when employment or job responsibilities change as detailed in Control AC-2.

Note: Control AC-2, Account Management, defines account authorization and expiration requirements for each type of account.

IA-5, Authenticator Management

a. Passwords and other authenticators must be treated as confidential information:
    1. Users are prohibited from sharing their password or authenticator with any other person.
    2. If the confidentiality of a password or authenticator is in doubt, it must be changed immediately.
b. Default or assigned passwords must be changed where feasible.
c. Passwords must be protected both in storage and in transit.
    1. When passwords are stored, they must be stored as a hash encrypted as specified by control IA-7.
    2. Where feasible, password hashes should be salted.
    3. Passwords must be encrypted when transmitted.
    4. Temporary passwords that are transmitted for the sole purpose of establishing a new password or changing a password can be excepted from the requirement to encrypt if it is a one-time transmission and the user must also change the password upon first logon.
d. Users will be directed to use a self-service password reset when they need to change their password. If a user is not able to perform a self-service reset, their identity must be verified before the password is changed.
    1. The password must be changed to a temporary password; and
    2. The user must change the temporary password at first logon (where applicable).
e. When automated password generation programs are utilized:
    1. Non-predictable methods of generation must be used;
    2. where feasible, systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system; and
    3. where feasible, password management and automated password generation systems must have the capability to maintain auditable transaction logs containing information such as:

        i. time and date of password change, expiration, and administrative reset;
        ii. type of action performed; and
        iii. source system (e.g. IP and/or MAC address) that originated the change request.
f. If a password or other authenticator is assumed to be compromised, the event must be reported as a security incident following control IR-6 Incident Reporting.
g. Where feasible, the following password complexity requirements will be implemented:
    1. The password must be 8 characters or more.
    2. The password may not be reused from the previous 6 passwords.
    3. Privileged accounts must have additional complexity.
h. Where feasible, user selected passwords must be checked to ensure that they meet complexity requirements by a password audit system.
i. The Information Resource Custodian responsible for a group/role account (e.g. a service account) will ensure that the password or authenticator is changed immediately when a user's authorization to use the account is revoked.
j. The expiration date must be three years or less for public key infrastructure authenticators (digital certificate private keys).

IA-6, Authenticator Feedback

a. Passwords fields must be masked.
b. Login error messages must not indicate which part of the username or password combination is incorrect.

IA-7, Cryptographic Module Authentication

a. At a minimum, cryptographic modules must use security functions approved in the Federal Information Processing Standards (FIPS) 140-3, see control SC-12.

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

a. Non-organizational users must be uniquely identified and authenticated before access is granted to an information resource as detailed in control AC-2.
    1. As specified in control AC-14, public websites, information kiosks and other situations where risk analysis demonstrates no need for individual accountability of users are exempt.

IA-11, Re-authentication

Information Resources must require periodic reauthentication for users and devices in the following circumstances or situations:

a. Where feasible, re-authentication must occur:
    1. When roles, authenticators, or credentials change.
    2. When a privileged function occurs.
b. Browser cookies used for binding authenticated sessions to System Offices-owned or managed information resources must expire in 5 days or less.
c. Workstations must be configured to automatically lock after 30 minutes of inactivity.
d. Multifactor authentication must be configured to force reauthentication every 5 days or less.

IA-11, Identity Proofing

a. Information Resource Custodians must verify a user's identity (identity proof) before granting access to a System Offices user account or any account with access to High Impact Information Resources.
b. User accounts on High Impact Information Resources must resolve to a unique individual.

Incident Response

IR-1, Incident Response Policy and Procedures

Incident Response Policy

The Texas A&M University System Offices recognizes that information security incident response policies and procedures are vital to reducing information security risks.

Purpose

The Incident Response Policy and associated controls describe the requirements for responding to and minimizing the impact of an information security incident impacting the System Offices.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners, and Custodians.

Compliance

Incident Response controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76, §202.73 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. The System Offices will follow the guidance of Texas A&M University System (TAMUS) Cybersecurity and the Texas Department of Information Resources (DIR) in responding to suspected information security incidents.
b. Prioritization of information security incidents will be based on the criticality of impacted resources, current and potential impact (e.g. unauthorized disclosure of confidential information, access to services, loss of revenue, and potential to spread to other information resources).

a. The System Offices ISO or their designee is responsible for:
    1. documenting and disseminating procedures that address the Incident Response family of controls for the information resources under their control; and
    2. ensuring that this policy and supporting procedures are periodically reviewed and updated.

IR-2, Incident Response Training

a. The System Offices Information Security Officer or their designee must ensure that information security incident response training is provided to appropriate staff. This training will be provided promptly for:
    1. new or existing staff that are assigned an information security role, and
    2. information Resource Custodians for High Impact Information Resources.

IR-3, Incident Response Testing

a. The System Offices Information Security Officer or their designee must ensure that the Information Security Incident Response Plan required by control IR-8 is tested periodically.

IR-4, Incident Handling

a. The System Offices Information Security Officer (SO ISO) or their designee is responsible for documenting information security incident handling procedures.
b. The SO ISO or their designee will coordinate the information security incident handling capability for the System Offices.
c. Information Resource Custodians in cooperation with A&M System Cybersecurity are responsible for:
    1. Implementing automated systems to facilitate information security incident detection, analysis, containment, eradication, and recovery.

    2. Coordinating with internal and external incident response providers to support information security incident handling.
d. Information security incident handling activities will be coordinated with contingency planning activities.
e. Information security incidents will end with an after-action review which includes recommendations for remediating the incident's root cause to prevent future similar occurrences.

IR-5, Incident Monitoring

a. Information security incidents are tracked and documented by the A&M System Cybersecurity and the Texas Department of Information Resources (DIR) through monthly reporting in the DIR Incident Management portal.

Note: Additional information resources monitoring requirements can be found in control SI-4, System Monitoring.

IR-6, Incident Reporting

a. Any user of System Offices-owned information resources may report illegal, disruptive, or suspicious activity to Information Technology personnel. Reportable incidents include:
    1. any events where the confidentiality, integrity, or availability of a System Offices-owned or managed information resource is potentially compromised;
    2. privacy incidents that do not impact the availability of information systems; and
    3. any incidents involving industrial control systems or operational technology.
b. Upon detection or notification, IT personnel will report suspected information security incidents to their IT leadership and to the Texas A&M University System Office of Cybersecurity.
c. Initial notification to the Office of Cybersecurity for security incidents must occur within four hours of discovery or notification to IT.
d. The Office of Cybersecurity will ensure reporting to System Offices that are required to be notified of an incident (to include the SOC, OGC, OCISO, OCIO, Internal Audit, Ethics & Compliance, and the Chancellor’s Office).
e. The Office of Cybersecurity will ensure all required reporting to the Texas Department of Information Resources (DIR) is accomplished in accordance with their prescribed schedule.

f. Reporting of information security incidents will follow the TAMUS incident notification matrix.
g. Summary reports of security-related events must be submitted to DIR as required by TAC §202.73.

IR-7, Incident Response Assistance

a. The Texas A&M University System Cyber Response Division will facilitate an effective response to suspected or confirmed information security incidents.

IR-8, Incident Response Plan

a. The System Offices Information Security Officer (SO ISO) or their designee will develop an information security incident response plan that:
    1. provides the System Offices with a roadmap for implementing its incident response capability;
    2. describes the structure and organization of the incident response capability;
    3. provides a high-level approach for how the incident response capability fits into the overall organization;
    4. meets the unique requirements of the System Offices, which relate to mission, size, structure, and functions;
    5. defines reportable incidents;
    6. provides metrics for measuring the incident response capability;
    7. defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    8. is reviewed and approved by System Offices Chief Information Officer.
b. The incident response plan will be distributed to personnel responsible for information system restoration;
c. The plan will be reviewed periodically and updated to address system changes or problems encountered during plan implementation, execution, or testing;
d. Changes to the plan must be communicated to incident response personnel
e. The plan must be protected from unauthorized disclosure and modification.

IR-9, Information Spillage Response

This control is required for information spills involving Confidential Information. It is optional for spills involving other data classifications.

a. The System Offices Information Security Officer (SO ISO) or their designee is responsible for coordinating a response to an information spill.

b. The specific information involved in the system contamination will be identified.

c. The event must be reported as required in the TAMUS incident notification matrix and control IR-6 Incident Reporting.

d. The contaminated system or system component will be isolated.

e. The information will be removed from the contaminated system or component.

f. Other systems or system components that may have been contaminated will be identified.

Maintenance

MA-1, System Maintenance Policy and Procedures

System Maintenance Policy

The Texas A&M University System Offices recognizes that system maintenance policies and procedures are vital to maintaining the confidentiality, integrity, and availability of information resources.

Purpose

The System Maintenance Policy and associated controls document the requirements to ensure that appropriate and timely maintenance is conducted to reduce the risks associated with unpatched resources.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners, and Custodians.

Compliance

System Maintenance controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the System Maintenance family of controls for the information resources under their control.
b. The SO ISO or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

c. Information Resource Custodians are responsible for ensuring that information resources are under manufacturer warranty / support for security patches and timely security patching is performed.
    1. Security patches categorized as “Critical” or "High" by the vendor should be installed within the next maintenance window or 30 days of release, whichever is lesser.
    2. Other security patches should be installed within 60 days of release.

Note: Where applicable under controls CM-3, and CM-3(2), change control procedures will be followed and security patches will be systematically tested, validated, and documented before implementation.

MA-2, Controlled Maintenance

a. Information Resource Custodians are responsible for scheduling, performing, documenting, and reviewing records of maintenance and repairs on information system components following manufacturer specifications.
b. Information Resource Owners or their designees should be notified of non-routine maintenance.
c. The System Offices Chief Information Officer or their designee must approve the removal of information resources or components for off-site maintenance or repairs.
d. Storage media containing data classified as Confidential must be removed or sanitized following control MP-6 before an information resource is removed for off-site maintenance, repair, surplus or other forms of disposal.
e. Security related functionality should be checked to ensure proper functionality after maintenance or patching is performed.
f. Patching and other forms of maintenance to information resources must be documented.

MA-4, Nonlocal Maintenance

Nonlocal actions include maintenance, support, diagnostics, or related actions by an individual who is not on the System Offices local network.

a. Nonlocal activities performed on System Offices information resources require prior approval by the System Offices Chief Information Officer or their designee.
b. Nonlocal activities must be documented.

MA-5, Maintenance Personnel

Maintenance personnel are individuals who perform hardware or software maintenance on System Offices information resources.

a. Information Resource Owners or their designees are responsible for:
    1. authorizing individuals who are allowed to perform maintenance on information resources; and
    2. maintaining a list of authorized maintenance organizations and personnel.
b. Information Resource Owners or their designees may decide to require supervision for activities performed by maintenance personnel.

Media Protection

MP-1, Media Protection Policy and Procedures

Media Protection Policy

The Texas A&M University System Offices recognizes that media protection policies and procedures are vital to reducing information security risks.

Purpose

The Media Protection Policy and associated controls document the minimum standards required to protect the data stored or processed by the System Offices.

All information resources that process, store, transmit or otherwise impact the confidentiality, integrity or accessibility of System Offices data must meet the Media Protection Policy and security controls.

Media includes both electronic media (e.g., hard drives, mobile devices including portable storage media such as USB memory sticks and portable computing and communications devices (e.g., laptop computers, tablets, smartphones, digital cameras, audio recording devices) and non-electronic media (e.g., paper).

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes all individuals involved in the handling of media that stores or processes data in the System Offices.

Compliance

Media Protection controls are implemented to ensure compliance with the Texas A&M University System Records Retention Schedule, Texas Government Code §441.187 Destruction of State Records, Texas Administrative Code §6.95 Final Disposition of Electronic State Records, the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the Media Protection family of controls for the information resources under their control.
b. The System Offices Information Security Officer (SO ISO) or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

MP-2, Media Access

a. Users should protect the confidentiality and integrity of data contained on removable storage media from unauthorized disclosure and modification throughout the life of the media, including disposal.
b. Access to removable storage media containing Confidential data should be restricted to authorized personnel using security mitigations commensurate with the risk and protected following control MP-7.

MP-3, Media Marking

a. Any media containing Confidential or sensitive personal information (as defined by TxBCC 521.002), must be marked electronically or physically using human-readable security attributes indicating the ownership, distribution limitations, handling caveats, and applicable data categorizations.
b. Removable electronic media stored in controlled areas does not have to be marked. System Offices IT controlled areas are the server room in the Moore / Connally Building and the Information Technology Services (ITS) office suite and SO leased racks at West Campus Data Center (WCDC) and Texas A&M University San Antonio (TAMUSA).

MP-6, Media Sanitization

Texas Government Code §441.187 Destruction of State Records and Texas Administrative Code §6.95 Final Disposition of Electronic State Records and the Texas A&M University System

Records Retention Schedule define requirements related to records retention and disposal that apply to the System Offices.

The following media sanitization controls apply to all System Offices Information resources that are leaving the custody of the System Offices, whether or not the media is considered removable.

a. Before leaving the custody of the System Offices, electronic media must be sanitized and destroyed in following the guidelines set by NIST SP 800-88.
b. The removal or destruction of electronic media must be documented. The documentation will include the following information:
    1. Date.
    2. Description of the item(s). If applicable, this should include the identification number(s) (e.g. serial number, or inventory number).
    3. The process and sanitization tools used to remove the data and/or the method of destruction.
    4. If applicable, the name of the organization the equipment was transferred to.
c. Prior to the destruction of any media, the Information Resource Owner or their designee should be consulted and reminded that media sanitization is not reversable. Owners or their designee are responsible for making a copy of any information that needs to be retained to another System Offices information resource before media is sanitized.

MP-7, Media Use

a. Removable electronic media (e.g. removable or portable hard drives, USB memory sticks, memory cards, etc.) containing Confidential data:
    1. Must be encrypted as specified in controls SC-12 and SC-13.
    2. Must have a duplicate copy of the information residing on System Offices-owned enterprise file storage.
    3. Must have a clearly designated owner who is accountable for ensuring that all applicable security controls are met.

Physical and Environmental Protection

PE-1, Physical and Environmental Protection Policies and Procedures

Physical and Environmental Protection Policy

The Texas A&M University System Offices recognizes that physical and environmental protection policies and procedures are vital to reducing information security risks.

Purpose

System Offices information resource facilities include data centers, and server rooms.

The Physical and Environmental Protection Policy and associated controls describe the requirements for managing risks associated with physical access to these facilities.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

Physical and Environmental Protection controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the Physical and Environmental Protection family of controls for the information resources under their control.

b. The SO ISO or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

Note: System Policy 29.01.03 documents physical protection requirements for data centers.

PE-2, Physical Access Authorizations

a. The System Offices Chief Information Officer or their designee is responsible for developing, approving, and maintaining a list of individuals who are authorized to access System Offices information resource facilities.
a. Access will be reviewed periodically.
b. Access will be removed promptly for individuals who no longer require access.
c. Full-time IT staff may escort maintenance personnel into information resource facilities without additional screening.

PE-3, Physical Access Control

a. Information Resource Custodians who are responsible for System Offices information resource facilities will ensure that physical access authorizations are enforced by:
    1. verifying individual access authorizations before granting access to the facility;
    2. controlling physical access to the facility using appropriate physical access control systems and safeguards based on risk management decisions;
    3. maintaining physical access audit logs as appropriate based on the criticality of the information resources being protected;
    4. escorting and monitoring visitors in restricted areas within the information resource facility;
    5. securing and maintaining an inventory of physical keys; and
    6. changing physical keys if keys are lost, or compromised, or when individuals with these keys are transferred or terminated.

PE-6, Monitoring Physical Access

a. Information Resource Custodians who are responsible for System Offices information resource facilities will:
    1. monitor physical access to detect and respond to physical security incidents at the facilities;
    2. review physical access logs periodically based on risk management decisions and upon the occurrence of an actual or potential indication of a security incident; and
    3. coordinate results of reviews and investigations with the A&M System Cybersecurity following controls IR-6 and IR-7 if there is an indication of an actual or potential security incident.

PE-8, Visitor Access Records

a. Information Resource Custodians will:
    1. maintain visitor access records to System Offices information resource facilities for one year; and
    2. review visitor access records periodically.

PE-12, Emergency Lighting

a. Information Resource Custodians will ensure that emergency lighting is installed in System Offices information resource facilities. The lighting must activate in the event of a power outage or disruption and cover emergency exits and evacuation routes within the facility.

PE-13, Fire Protection

a. Information Resource Custodians will ensure that System Offices information resource facilities are protected by fire suppression and detection system.

PE-14, Temperature and Humidity Controls

a. Information Resource Custodians will ensure that temperature and humidity are monitored and kept at acceptable levels within System Offices information resource facilities.

PE-15, Water Damage Protection

a. Information Resource Custodians will ensure that infrastructure is protected from water damage in System Offices information resource facilities.

PE-16, Delivery and Removal

a. Information Resource Custodians will ensure that appropriate authorization and monitoring are in place for the delivery and removal of information system components at information resource facilities. Delivery and removal of components must be documented.

PE-17, Alternate Work Site

a. System Policy 33.06.01 documents requirements for alternate work locations.

b. Control AC-17, Remote Access defines Remote access security requirements.

c. The effectiveness of the controls in AC-17 will be assessed anytime a change to the controls is made.

d. Control IR-6, Incident Reporting defines information security reporting requirements.

Planning

PL-1, Planning Policy and Procedures

Security Planning Policy

The Texas A&M University System Offices recognizes that information security planning policies and procedures are vital to reducing information security risks.

Purpose
The Planning Policy and associated controls describe the requirements for documenting security and privacy plans and rules of behavior for information resource users.

Scope and Roles
This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO).

Compliance
Security Planning controls are implemented to ensure compliance with Title 1 Texas Administrative Code §202.73(a), and Texas Government Code §2054.133, the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76, and Texas A&M University System Policy 29.01.03, Information Security.

Implementation
The SO ISO or their designee is responsible for:

a. documenting and disseminating procedures that address the Security Planning family of controls; and
b. ensuring that this policy and supporting procedures are periodically reviewed and updated.

PL-2, System Security and Privacy Plans

a. Information Resource Owners or their designees must develop a System Security and Privacy Plan for each High Impact Information Resource that:
    1. defines the system components that are authorized for operation by the Information Resource Owner (see control CM-8);
    2. describes the business process(es) supported by the information resource;
    3. identifies the individuals that fulfill system roles and responsibilities;
    4. identifies the information types processed, stored, and transmitted by the system (see Texas A&M University System Data Classification Standard);
    5. provides the security categorization of the system, including supporting rationale (see control RA-2, Security Categorization);
    6. describes any specific threats to the system that are of concern to the organization;
    7. provides the results of a privacy risk assessment for systems processing personally identifiable information;
    8. describes and any dependencies on or connections to other systems or system components;
    9. provides an overview of the security and privacy requirements for the system;
    10. identifies any relevant control baselines or overlays, if applicable; and
    11. describes the unique controls in place or planned that exceed the common security controls applied to all System Offices information resources, including a rationale for any exceptions or tailoring decisions.
b. Information Resource Owners or their designees are responsible for:
    1. periodically reviewing and updating the plans as changes occur to the information resource; and
    2. distributing the plans and communicating changes as appropriate to the System Offices Information Security Officer (SO ISO) and other authorized individuals;
c. The SO ISO or their designee is responsible for reviewing the plans. As detailed in control PL-1, security and privacy plans are included in the annual report on the information security program delivered to the System Offices Chief Information Officer and submitted biannually to Department of Information Resources (DIR) as part of the System Offices Information Security Plan.
d. System security and privacy plans must be protected from unauthorized disclosure and modification.

PL-4, Rules of Behavior

a. Use of system resources is documented in Texas A&M University System Policies 29.01 and 33.04. Acceptable Use Standards are documented in the System Offices Statement of Responsibility (SOR). These documents provide the rules that govern the appropriate use of all System Offices-owned or maintained information resources for System Offices users, including employees, contractors, and other system users.
b. Users must sign the SOR before receiving an account. By signing, the user acknowledges their understanding of the Acceptable Use Standards, rules of behavior and their responsibilities as a user of System Offices information resources.
c. The System Offices Information Security Officer or their designee is responsible for reviewing and updating the SOR and Acceptable Use Standards periodically.
d. Individuals who have signed a previous version of the SOR and Acceptable Use Standards must read and resign when it is updated.

Program Management

PM-1, Information Security Program Plan

System Offices Information Security Program and Plans

The Texas A&M University System Offices recognizes that the information security program and plans are vital to reducing information security risks.

Purpose

The Information Security Program Plan is a formal document that provides an overview of the security requirements for the System Offices information security program. This family of controls describes requirements related to the Information Security Program Plan.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO).

Compliance

The Information Security Program Plan and associated controls are implemented to ensure compliance with Title 1 Texas Administrative Code (TAC) §202.70, §202.71, §202.73, §202.74, Texas Government Code §2054.133, the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by TAC §202.76, and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. The SO ISO or their designee is responsible for:
    1. documenting and disseminating procedures that address the Information Security Program Plan family of controls;

2. developing an Information Security Program Plan that satisfies the requirements of TAC §202, as required by §202.71, §2054.133 and Texas A&M University System Policy 29.01.03;
3. annually reviewing and updating the Information Security Program Plan informed by ongoing risk assessments and considering changes in business, technology, threats, incidents, and System Offices priorities;
4. delivering the System Offices Information Security Program Plan to DIR before June 1 of each even-numbered year as required by §202.73 and §2054.133; and
5. ensuring that the Information Security Program Plan is independently reviewed every two years at a minimum as required by TAC §202.70, §202.71, and §202.76.

b. The System Offices Information Security Program Plan must be approved by the Texas A&M University System Chancellor, or their designee as required by TAC §202.73, and Texas A&M University System Policy 29.01.03.
c. The Information Security Program Plan must be protected from unauthorized disclosure and modification.

PM-2, Information Security Program Leadership Role

a. The System Offices Information Security Officer is the designated senior Information Security Officer and is responsible for all requirements outlined Texas Government Code §2054.136, Texas Administrative Codes §202.70, §202.71, and Texas A&M University System Policy 29.01.03.

PM-3, Information Security and Privacy Resources

a. As required by Texas Administrative Code §202.70, the System Offices Chief Information Officer will allocate resources for ongoing information security remediation, implementation and compliance activities that reduce risk to an acceptable level. Information security budgeting and planning are integrated into the overall System Offices information resources budgeting strategy.

PM-4, Plan of Action and Milestones Process

a. The System Offices Information Security Officer or their designee is responsible for developing and maintaining a plan of action and milestones for the information security program.
b. The plan of action and milestones will be included in the annual Information Security Program Plan and included in reports as documented in controls PL-1, and PM-1.

PM-5, Information System Inventory

a. The Office of Information Technology will designate a system of record for the inventory of information systems, network-attached technology, and cloud computing services owned or operated by the System Offices.
b. At a minimum, the inventory must record a unique identifier (e.g. serial number or system name), owner, custodian, a description of the information system's function or major application, and the highest level of data categorization stored/processed (see control RA-2).
c. Information Resource Owners or their designees are responsible for maintaining an inventory of information resources under their control.

PM-6, Information Security Measures of Performance

a. The System Offices Information Security Officer or their designee is responsible for developing, monitoring, and reporting on the results of information security measures of performance.
b. Measures of performance will be included in the annual Information Security Program Plan (see controls PL-1, and PM-1).

PM-7, Enterprise Architecture

a. The System Offices enterprise information system architecture will be developed with consideration for information security and the resulting risk to operations, assets, individuals, and other organizations.
b. Information security imperatives, including Texas Administrative Code §202.21, Texas A&M University System Policy 29.01.03 and this catalog, will be referenced and followed when designing and implementing the enterprise architecture.

PM-9, Risk Management Strategy

The System Offices Information Security Officer (SO ISO) or their designee is responsible for:

a. developing a comprehensive strategy to manage:
    1. risks associated with the operation of the organization's information resources,
    2. privacy risk to individuals resulting from the authorized processing of personally identifiable information; and
b. Implementing the risk management strategy across the organization; and
c. ensuring that this strategy is periodically reviewed and updated.

PM-10, Authorization Process

The System Offices Information Security Officer (SO ISO) or their designee is responsible for:

a. ensuring there are appropriate authorization processes to manage the security and privacy state of information resources; and
b. designating individuals who are responsible for types of authorizations.
c. Authorization processes should document implementation details for control CA-6, Security Authorization and be consistent with the organization's risk tolerance documented in the Risk Management Strategy (see control PM-9).

PM-14, Testing, Training, Monitoring

a. The System Offices Information Security Officer is responsible for developing and maintaining organization plans for security testing, training, and monitoring.
b. A&M System Cybersecurity will provide security monitoring for the System Offices network.

Note: The Awareness and Training family of controls provide specific requirements for information security training.

PM-15, Security and Privacy Groups and Associations

Establish and institutionalize contact with selected groups and associations within the security and privacy communities. The purpose of these contacts is to:

a. facilitate ongoing security and privacy education and training for organizational personnel;

b. maintain currency with recommended security and privacy practices, and technologies; and

c. share current security and privacy information, including threats, vulnerabilities, and incidents (see control PM-16).

PM-16, Threat Awareness Program

a. The System Offices Information Security Officer (SO ISO) or their designee is responsible for sharing threat awareness information and cross-organization information sharing.

b. Threat awareness information that may impact the System Offices will be disseminated as operational security permits.
c. The SO ISO or their designee will determine the appropriate dissemination method, content, and timing of such information.

Personnel Security

PS-1, Personnel Security Policy and Procedures

Personnel Security Policy

The Texas A&M University System Offices recognizes that personnel security policies and procedures are vital to reducing information security risks.

Purpose

The Personnel Security Policy and associated controls document the requirements for managing risks associated with personnel including hiring, termination, transfer, third-party personnel, and disciplinary action.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes all individuals involved in hiring and personnel management as well as Information Resource Owners and the System Offices Information Security Officer (SO ISO).

Compliance

Personnel Security controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M System Regulation 29.01.03, Information Security.

Implementation

The SO ISO or their designee is responsible for:

a. documenting and disseminating procedures that address the Personnel Security family of controls.

b. ensuring that this policy and supporting procedures are periodically reviewed and updated.

PS-2, Position Risk Designation

a. The System Offices Information Security Officer or their designee in cooperation with Information Resource Owners and Human Resources personnel, will assign a risk designation to all organizational positions.
b. Position risk designations must be reviewed periodically.

PS-3, Personnel Screening

a. As required by Texas A&M University System Policy 33.99.14, all current employees and employee candidates must be screened through the human resources hiring process for a criminal background.
b. Rescreening may be performed based on a risk determination for changes in access or roles and responsibilities or as required by human resource policies.
c. The System Offices Information Security Officer may perform additional personnel screening for users with access to High Impact Information Resources based on a risk determination of the proposed access.

PS-4, Personnel Termination

a. Managers, account sponsors and Human Resources are responsible for notifying Information Technology as soon as feasible in the event of a termination.
b. Upon termination of employment or the end date for a sponsored account:
    1. The manager or sponsor must retrieve all System Offices information system-related property.
    2. The user's account and access to System Offices information resources must be disabled.
    3. Upon request from the department head, IT will provide the supervisor, account sponsor, or other appropriate personnel with access to email, files and other

electronic records created by the terminated employee that are stored on System Offices information resource for no more than 30 days.

4. Access can be extended based on sufficient business need or for legal requirements. Requests should document a justification for the extension and the length of the extension.

PS-5, Personnel Transfer

a. Access authorizations are to be modified appropriately as an account holder's employment or job responsibilities change.
c. Managers, account sponsors and Human Resources are responsible for notifying Information Technology as soon as feasible in the event of a transfer.
b. The manager in conjunction with Information Resource Owners and IT are responsible for reviewing the employee's information resource access to ensure that access is appropriate for the duties to be performed.

PS-6, Access Agreements

Information resource access agreements may include a statement of responsibility, acceptable use agreements, nondisclosure agreements (NDAs), facility access agreements, and conflict of interest agreements.

a. The System Offices Information Security Officer or their designee, is responsible for developing access agreements for System Offices information resources.
b. Access agreements should be reviewed periodically.
c. Controls AC-2 and PL-4, document requirements for users to agree to and sign the Statement of Responsibility, Acceptable Use Standards, and rules of behavior.

PS-7, External Personnel Security

External personnel or third-party providers include contractors, vendors, suppliers, managed service providers, and other organizations providing information technology services such as:

information system development, outsourced application support, or information security services.

a. External personnel must comply with the System Offices information security policies and controls.
b. System Offices staff overseeing the work of third parties are responsible for:
    1. communicating and enforcing applicable laws, as well as System Offices policies, and procedures, and
    2. monitoring provider compliance.
c. Third parties must notify the information resource owner or their designee of any transfers or terminations of external personnel.

PS-8, Personnel Sanctions

a. Information security policies and procedures are enforced by Texas A&M University System (TAMUS) Policy 29.01.03 which includes the following statement for staff responsibilities: “Users of system or member information resources who fail to comply with this regulation and/or system and member information security requirements are subject to disciplinary action, up to and including termination of employment.”
b. TAMUS Policy 32.02.02 documents procedures for employee discipline and dismissal.

Personally Identifiable Information Processing and Transparency

PT-3, Personally Identifiable Information Processing Purposes

a. All System Offices users are responsible for reducing, and eliminating where possible, the collection and/or use of sensitive personal information in information resources under the control of the System Offices.

Risk Assessment

RA-1, Risk Assessment Policy and Procedures

Risk Assessment Policy

The Texas A&M University System Offices recognizes that risk assessment policies and procedures are vital to reducing information security risks and meeting our legal requirements for protecting confidential information.

Purpose

The Risk Assessment Policy and associated controls describe the requirements for identifying, analyzing, and managing information security risks associated with the System Offices information and information resources.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

Risk Assessment controls are implemented to ensure compliance with Title 1 Texas Administrative Code (TAC) §202.75, §202.74, and the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by TAC §202.76 and Texas A&M University System Policy 29.01.03 – Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the Risk Assessment family of controls for the information resources under their control.
b. The SO ISO or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

RA-2, Security Categorization

a. Information Resource Owners or their designee are responsible for determining and documenting the data classification category for each information resource under their control following The Texas A&M University System data classification standard.
b. Information Resource Owners or their designee are responsible for maintaining an accurate inventory of information resources that store or process data classified as Confidential (see control PM-5).
c. Information Resource Owners will work to reduce, and eliminate where possible, the collection and/or use of sensitive personal information in information resources under the control of the System Offices.
d. The final determination of classification categories may be subject to review by the System Offices Information Security Officer.

RA-3, Risk Assessment

a. Texas A&M University System (TAMUS) Policy 29.01.03 requires an annual information security risk assessment that complies with Texas Administrative Code (TAC) §202.75. Information Resource Custodians must conduct an annual risk assessment for each High Impact Information Resource including:
    1. Identifying threats to and vulnerabilities in the system;
    2. Determining the likelihood and magnitude of harm from unauthorized use, disclosure, disruption, modification, or destruction. Risks and impacts will be ranked as either "High", "Moderate," or "Low."
b. The assessment results, vulnerability reports and the inventory of High Impact Information Resources must be provided to the System Offices Information Security Officer (SO ISO) for review as required by TAC §202.75, and A&M System Cybersecurity as required by TAMUS Policy 29.01.03.
c. Approval of the security risk acceptance, transfer, or mitigation decisions are the responsibility of:
    1. The SO ISO or their designee(s), in coordination with the information resource owner, for systems identified with Low or Moderate residual risk.
    2. The Chancellor or their designee for all systems identified with a High residual risk.
d. Assessment results and risk decisions will be used as a basis for the System Offices Information Security Program as required by §TAC 202.74. See controls PL-2, PM-1, PM-4, PM-6, and PM-9.

e. The schedule of the future risk assessments will be documented as required by TAC §202.75.
f. Information security risk assessments may be excepted from disclosure under Texas Government Code §2054.077(c) or Texas Government Code §552.139.

RA-3(1), Supply Chain Risk Assessment

a. The System Offices Information Security Officer (SO ISO) or their designee is responsible for assessing supply chain risks associated with High Impact Information Resources, and;

b. updating the supply chain risk assessment periodically, when there are significant changes to the System Offices technology supply chains, or when changes, or other conditions may necessitate a change in the supply chain.

RA-5, Vulnerability Scanning

a. The System Offices Information Security Officer (SO ISO) or their designee will ensure that all System Offices information resources are scanned for security vulnerabilities periodically, or when significant new vulnerabilities potentially affecting the system are identified.
b. Vulnerability monitoring tools should be implemented to identify systems connected to the network, software flaws, and improper configurations and to measure the impact of vulnerabilities.
c. Information Resource Owners and Custodians should be notified of vulnerabilities that are found. Custodians are responsible for ensuring that identified risks are fixed or mitigated in a timely manner.
    1. If identified vulnerabilities are not remediated, the affected information resource may be isolated or disconnected from the network.
    2. Vulnerabilities with a VPR and/or CVSS score greater than or equal to 7.0 ("High" or "Critical" severity):

        i. must be remediated within seven days of notification to maintain open ports through the network firewall; and
        ii. must be remediated within 30 days of notification to maintain access to the network.
    3. Information resources having security vulnerabilities with a VPR and/or CVSS score less than 7.0 ("Medium" or "Low" severity):
        i. must be remediated within 30 days of notification to maintain open ports through the network firewall; and
        ii. must be remediated within 60 days of notification to maintain access to the network.
d. Vulnerability and network scanning may only be conducted by the System Offices Information Security Officer (SO ISO), A&M System Cybersecurity or an entity authorized by the SO ISO or their designee.

RA-7, Risk Response

Information Resource Custodians are responsible for responding to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance and system criticality.

System and Services Acquisition

SA-1, System and Services Acquisition Policy and Procedures

System and Services Acquisition Policy

The Texas A&M University System Offices recognizes that system and services acquisition policies and procedures are vital to reducing information security risks.

Purpose

The System and Services Acquisition Policy and associated controls help to ensure that systems, system components and services that are acquired are compliant with System Offices information security standards, are compatible with existing information resources, have sufficient documentation, and are an efficient use of funds.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Chief Information Officer (SO CIO), the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

System and Services Acquisition controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. The SO CIO or their designee is responsible for:

1. documenting and disseminating procedures that address the System and Services Acquisition family of controls;
2. ensuring that this policy and supporting procedures are periodically reviewed and updated; and
3. coordinating the purchase of information resources, regardless of the funding source.

SA-2, Allocation of Resources

a. As required by Texas Administrative Code §202.70, the System Offices Information Security Officer (SO ISO) or their designee will:
    1. determine information security requirements for information resources or services as part of the System Offices strategic planning process;
    2. determine, document, and allocate resources required to adequately protect information resources as part of the capital planning process; and
b. The SCIO or their designee will establish a discrete line item for information security in the System Offices budget.

SA-3, System Development Life Cycle

a. The System Offices Information Security Officer or their designee is responsible for reviewing the data security requirements and specifications of any new information systems or services that process and/or store data classified as Confidential.

SA-4, Acquisition Process

a. Information Resource Owners or their designees, in conjunction with procurement and contracting personnel, must include information security requirements in all information resource acquisition contracts based on an assessment of risk and in accordance with applicable laws including Texas Administrative Code (TAC) §202.77, and Texas A&M University System Policies including 25.07, 25-07-01, and 25-07-03.

1. TAC §202.77 requires compliance with the Texas Risk and Authorization Management Program (TX-RAMP) for new and renewed contracts for cloud computing services. See Texas Department of Information Resources guidance.

SA-5, Information System Documentation

a. Information Resource Custodians must obtain or develop administrator documentation for each information resource under their authority that describes:
    1. how to securely install, configure, operate, and maintain the information resource;
    2. how to effectively use security and privacy functions; and
    3. known vulnerabilities related to the configuration and use of administrative functions.
b. Information Resource Custodians must obtain or develop user documentation for each information resource under their authority that describes:
    1. how to use user-accessible security and privacy functions; and
    2. how to use the system in a more secure manner and protect individual privacy.
c. Documentation related to the secure configuration, effective use, or known vulnerabilities will be maintained by the Information Resource Custodian and made available to users and/or administrators, as appropriate.

SA-8, Security and Privacy Engineering Principles

Information Resource Custodians should apply systems security and privacy engineering principles commensurate with a system's risks and criticality. These should be applied throughout the system's lifecycle: specification, design, development, implementation, and modification.

SA-9, External Information System Services

a. Information Resource Owners or their designees are responsible for:
    1. requiring that providers of external information system services comply with System Offices information security controls, and applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance.
    2. defining and documenting oversight and user roles and responsibilities for external information system services; and
    3. employing processes and procedures to monitor security control compliance by external service providers on an ongoing basis (i.e., annual risk assessment process).

SA-10, Developer Configuration Management

a. System developers are responsible for following a configuration change control process as defined by the Configuration Management family of controls.

SA-11, Developer Testing and Evaluation

The organization developer/architect of the system, system component, or system service, at all post-design stages of the system development life cycle, will be responsible to:

a. Develop and implement a plan for ongoing security and privacy assessments;

b. Perform [unit, integration, system, regression] testing/evaluation at regular intervals;

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation as appropriate.

SA-22, Unsupported System Components

The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and

b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

System and Communications Protection

SC-1, System and Communications Protection Policy and Procedures

System and Communications Protection Policy

The Texas A&M University System Offices recognizes that system and communications policies and procedures are vital to reducing information security risks.

Purpose

The System and Communications Protection Policy and associated controls document the minimum standards required to protect System Offices communications within the internal network, across the Internet and through other forms of data transmission.

Scope and Roles

This policy applies to information resources owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

System and Communications Protection controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

a. Information Resource Owners or their designees are responsible for documenting and disseminating procedures that address the System and Communications Protection family of controls for the information resources under their control.

b. The SO ISO or their designee is responsible for ensuring that this policy and supporting procedures are periodically reviewed and updated.

SC-5, Denial of Service Protection

a. High Impact Information Resources that are highly susceptible to a denial-of-service attack should reside behind network defense systems that are able to reduce the risk of such an attack where feasible.

SC-7, Boundary Protection

a. The System Offices Information Security Officer (SO ISO), or their designee, is responsible for:
    1. ensuring that monitoring and controls are in place for the external boundary of the network and at key internal boundaries;
    2. ensuring that publicly accessible system components are logically separated from internal System Offices networks (e.g. residing in a demilitarized zone, or on an external network); and
b. All connections between System Offices information resources and the internet must be provided by the Office of Information Technology or an Internet service provider authorized by the System Offices Chief Information Officer (SO CIO) or their designee. Individual departments are not allowed to establish independent internet connectivity without the approval of the SO CIO.
    1. Users working from remote locations are exempt from this control.
c. Information resources should employ controls such as firewalls to control inbound and outbound traffic where feasible.

SC-8, Transmission Confidentiality and Integrity

a. Data transmitted over a public network (e.g. the Internet), should be encrypted where feasible.

b. Data classified as Confidential that is transmitted over a public network must be encrypted following controls SC-12 and SC-13.

SC-12, Cryptographic Key Establishment and Management

a. Cryptographic keys will be established in accordance with the Commercial National Security Algorithm Suite (CNSA).

SC-13, Cryptographic Protection

a. Data classified as Confidential must be protected with appropriate encryption at all times, both at rest and in transit.
b. Storing System Offices data on removable storage media is discouraged. Confidential data must be encrypted if copied to or stored on removable media.
c. All System Offices servers, desktop, laptop, and mobile devices must use full-disk encryption where feasible.

SC-15, Collaborative Computing Devices

Collaborative communication devices include speaker phones, video cameras, networked screens, networked white boards, and other teleconferencing equipment.

a. Collaborative communication devices in sensitive work areas must have remote activation methods disabled. Administrative access to the device must be restricted to authorized IT personnel.

    1. An exception to this control is approved for communication devices in public conference rooms.
b. Collaborative communication devices should have an explicit indication of use. Users should be aware when these devices are activated.

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

a. The System Offices DNS must provide:
    1. data origin and integrity verification assurances (e.g. DNSSEC), and
    2. an indication of the security status of child zones under the ad.tamus.edu domain. (e.g. DNS delegation signer (DS) resource records).
b. DNS servers must be configured so zone transfers are only allowed to a list of trusted servers.

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

a. System Offices information resources must use an approved authoritative DNS source that provides a mechanism for verifying data origin and integrity (e.g. through DNSSEC) where feasible.
b. A client-based secure DNS resolution client is required on System Offices controlled endpoints where feasible.

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

a. All components of the System Offices DNS resolution services must be fault tolerant.
b. Split DNS should be used to prevent leaking internal system and IP information to external non-TAMUS clients.
    1. DNS servers with internal roles should only process name and address resolution requests from internal System Offices Information Resources.
    2. DNS servers with external roles should only process name and address resolution information requests from external clients (e.g., DNS requests from the Internet).

SC-39, Process Isolation

a. System Offices information resources must use operating systems that support process isolation where feasible.
b. Operating systems will be configured to enable data execution prevention where feasible.

System and Information Integrity

SI-1, System and Information Integrity Policy and Procedures

System and Information Integrity Policy

The Texas A&M University System Offices recognizes that system and information integrity policies and procedures are vital to reducing information security risks.

Purpose

The System and Information Integrity Policy and associated controls document the minimum standards required to protect the confidentiality, integrity and availability of information resources and data. Requirements are defined for patches and updates, malicious code protection, information system monitoring, security alerts, information handling and retention.

Scope and Roles

This policy applies to Information Resources and data owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

System and Information Integrity controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

The SO ISO or their designee is responsible for:

a. documenting and disseminating procedures that address the System and Information Integrity family of controls; and
b. ensuring that this policy and supporting procedures are periodically reviewed and updated.

SI-2, Flaw Remediation

a. Information Resource Custodians are responsible for:
    1. identifying, reporting, and correcting information resource security flaws as described in controls IR-6 and RA-5;
    2. testing software and firmware updates related to security flaw remediation for effectiveness and potential side effects before installation as described in control CM-3;
    3. installing security-relevant software and firmware updates within timelines as specified in controls MA-1, MA-2; and
    4. incorporating security flaw remediation into the configuration management process as specified in control CM-3.

SI-3, Malicious Code Protection

a. System Offices information resources must be patched and updated following control MA-1.
    1. Software and hardware that is no longer supported by the manufacturer is not permitted. Exceptions require approval by the System Offices Information Security Officer (SO ISO) or their designee and mitigating controls.
b. Email attachments and shared files should be scanned for malicious code before they are opened or accessed.
c. System Offices information systems must use endpoint protection software to detect and remove or quarantine malicious code (e.g. anti-virus software) where feasible. Exceptions for servers or workstations require approval by SO ISO or their designee and mitigating controls.
    1. The automatic update feature must be enabled in software that guards against malicious code where feasible.

d. Personally owned devices that connect to networks within the same boundary as High Impact Information Resources must employ endpoint protection software or suitable compensating controls, based on assessed risk.

SI-4, Information System Monitoring

a. The System Offices Information Security Officer or their designee is responsible for implementing information security monitoring.
b. High and Moderate Impact information resources must be monitored to detect:
    1. attacks and indicators of potential attacks;
    2. unauthorized local, network and remote connections;
    3. unauthorized access or use; and
    4. attempts to deny service or degrade the performance.
c. Logs and other data generated by security monitoring should be reviewed periodically based on risk management decisions.
d. Any significant security issues discovered, or signs of unauthorized activity will be reported following control IR-6.

SI-5, Security Alerts, Advisories, and Directives

a. The System Offices Information Security Officer (SO ISO) or their designee, is responsible for:
    1. receiving information security alerts and advisories from established resources including A&M System Cybersecurity, Texas Department of Information Resources (TxDIR), Multistate Information Sharing and Analysis Center (MS-ISAC), and United States Computer Emergency Response Team (US-CERT) and other internal external sources;
    2. identifying and evaluating alerts and advisories for reporting security threats that may impact the System Offices;
    3. communicating internal security alerts, advisories, and directives as necessary;
    4. determining required response activities with established time frames that will be specified in a directive to the Information Resource Custodian(s) who are impacted; and

5. ensuring appropriate action is completed.

SI-10, Information Input Validation

Information systems should check the validity of information inputs by:

a. Checking the valid syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values).

b. Prescreen and validate inputs before passing to interpreters to prevent the content from being unintentionally interpreted as commands.

SI-12, Information Output Handling and Retention

a. All System Offices information must be handled in accordance with the Texas A&M University System record retention schedule and data classification standard, and relevant legal requirements.

Supply Chain Risk Management

SR-1, Policy and Procedures

Supply Chain Risk Management Policy

The Texas A&M University System Offices recognizes that information resource supply chain policies and procedures are vital to reducing information security risks.

Purpose

The Supply Chain Risk Management Policy and associated controls document the minimum standards required to manage risks associated with using information resources from external providers. Requirements are defined for supply chain risk management, acquisition, notification agreements and component disposal.

Scope and Roles

This policy applies to Information Resources and data owned or managed by the Texas A&M University System Offices. The intended audience includes the System Offices Information Security Officer (SO ISO), Information Resource Owners and Custodians.

Compliance

Supply Chain Risk Management controls are implemented to ensure compliance with the Texas Department of Information Resources (DIR) Security Control Standards Catalog as required by Title 1 Texas Administrative Code §202.76 and Texas A&M University System Policy 29.01.03, Information Security.

Implementation

The SO ISO or their designee is responsible for:

a. Documenting and disseminating procedures that address the Supply Chain Risk Management family of controls;

b. Designate an individual to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. ensuring that this policy and supporting procedures are periodically reviewed and updated.

SR-2, Supply Chain Risk Management Plan

The System Offices Information Security Officer (SO ISO) or their designee is responsible for:

a. Developing a Supply Chain Risk Management Plan for managing supply chain risks to organizational systems;

b. Reviewing and updating the plan periodically, to address changes in threats, the organization or environment. No longer than every two years; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-3, Supply Chain Controls and Processes

The System Offices Information Security Officer (SO ISO) or their designee is responsible for:

a. The organization establishing a process to identify and address weaknesses in the supply chain elements and processes of High Impact Information Resources in coordination with Information Resource Custodians.

b. Employing the following controls to protect against supply chain risks to the system, system component, or service and to limit the harm or consequences from supply chain-related events:

    1. CA-2, Control Assessments
    2. MA-2, Controlled Maintenance
    3. SA-4, Acquisition Process
    4. SA-9, External System Services

5. SR-12, Component Disposal

c. Documenting the supply chain processes and controls in the organization's security plan.

SR-5, Acquisition Strategies, Tools, and Methods

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: the organization shall consult with A&M System Cybersecurity pertaining to supply chain risks.

SR-8, Notification Agreements

The procuring party, in consultation with the System Offices ISO shall establish notification agreements and procedures with external entities. The notification of supply chain compromises includes security incidents, privacy breaches and the notification of assessment or audit results.

SR-12, Component Disposal

The organization resource owner will dispose of documentation, tools, and system components using techniques that prevent the disclosure of sensitive information.

The Texas A&M University System Offices Information Security Control Standards Catalog is approved by:

_____	System Chief Information Officer
Name	Title
_____	_____
Signature	Date

_____	System Chief Information Security Officer
Name	Title
_____	_____
Signature	Date

Update Log

Date	Description	Change Made By	Approved By
1/2/2023	Per Governor's Directive on TikTok: Added AC-19 e., MDM requirement Added SC-21 b., secure client-based DNS for endpoints requirement	Jeremy Tarpley	Terry Tatum
09/06/23	Updated required Controls for 07/20/2023	Andrew Fulton	Terry Tatum
11/14/23	Cleaned up Master Document and Updated required FY23 Approved Controls	Andrew Fulton	Terry Tatum
5/01/24	Cleaned up terminology, roles and responsibilities, Updated	Andrew Fulton	