Access Control .............................................................. Page 1
Awareness & Training ....................................................... Page 6
Audit and Accountability .................................................. Page 8
Security Assessment and Authorization ................................ Page 11
Configuration Management .............................................. Page 14
Contingency Planning ...................................................... Page 17
Identification and Authentication ....................................... Page 20
Incident Response .......................................................... Page 23
Maintenance ..................................................................... Page 26
Media Protection .............................................................. Page 28
Network Management ...................................................... Page 30
Physical and Environmental Protection ............................... Page 32
Planning ............................................................................ Page 35
Program Management ...................................................... Page 39
Personnel Security ............................................................ Page 41
Risk Management ............................................................ Page 44
System and Services Acquisition .......................................... Page 46
System and Communications Protection ............................. Page 49
Server Management .......................................................... Page 52
System and Information Integrity ........................................ Page 54
Information Technology Glossary ....................................... Page 57
Access Control Policy

Purpose: The purpose of this policy is to define information security controls around access control.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Access controls by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Access Control Policy

Authority - DIR Controls Catalog (DIR CC): AC-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Access Control policy and associated access controls; and

3.1.2 Review and update access control procedures at an institution-defined frequency.

4. Account Management

Authority - DIR CC: AC-2, TAC 202.72

4.1 Component institutions must:

4.1.1 Identify and document, in consultation with the institution’s ISO and IRM, the types of information system accounts that support organizational missions and business functions;

4.1.2 Assign account manager responsibilities for information system accounts to the respective information owner;

4.1.3 Establish conditions for group and role membership;

4.1.4 Require the respective information owner to specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
4.1.5 Require approval from the information owner for requests to create information system accounts;

4.1.6 Require the respective information custodian to create, enable, modify, disable, and remove information system accounts in accordance with institution-defined procedures;

4.1.7 Require the respective information custodian to monitor the use of information system accounts;

4.1.8 Notify account managers:
   4.1.8.1 When accounts are no longer required;
   4.1.8.2 When users are terminated or transferred; and
   4.1.8.3 When individual information system usage or need-to-know changes;

4.1.9 Require that the respective information owner authorize access to the information system based on:
   4.1.9.1 A valid access authorization;
   4.1.9.2 Intended system usage; and
   4.1.9.3 Other attributes as required by the institution or associated missions/business functions;

4.1.10 Require respective information custodians to review accounts for compliance with account management requirements at an institution-defined frequency; and

4.1.11 Require respective information owners and information custodians to establish processes for reissuing shared/group account credentials (if deployed) when individuals are removed from a group.

5. **Account Enforcement**
   Authority - DIR CC: AC-3

   5.1 Component institutions must ensure that information systems enforce approved authorizations for logical access to information and system resources in accordance with applicable, institution-defined access control policies.

6. **Separation of Duties**
   Authority - DIR CC: AC-5

   6.1 Component institutions must:
   
   6.1.1 Ensure that duties of individuals are appropriately separated based on institution-defined criteria;
   
   6.1.2 Document separation of duties of individuals; and
   
   6.1.3 Define information system access authorizations to support separation of duties.

7. **Unsuccessful Logon Attempts**
   Authority - DIR CC: AC-7

   7.1 Component institutions must ensure that each information system:
7.1.1 Enforces an institution-defined limit of consecutive, invalid logon attempts by a user during an institution-defined time period; and

7.1.2 Automatically performs one of the following actions when the maximum number of unsuccessful attempts is exceeded:

7.1.2.1 Locks the account or node for an institution-defined time period;

7.1.2.2 Locks the account or node until released by an administrator; or

7.1.2.3 Delays the next logon prompt according to an institution-defined delay algorithm.

8. System Use Notification
Authority - DIR CC: AC-8

8.1 Component institutions must ensure that each information system:

8.1.1 Displays to human users at logon interfaces an institution-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

8.1.1.1 Users are accessing an institutional information system;

8.1.1.2 Information system usage may be monitored, recorded, and subject to audit;

8.1.1.3 Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

8.1.1.4 Use of the information system indicates consent to monitoring and recording;

8.1.2 Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

8.1.3 For publicly accessible systems that do not have logon interfaces:

8.1.3.1 Displays system use information under institution-defined conditions before granting further access;

8.1.3.2 Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

8.1.3.3 Includes a description of the authorized uses of the system.
9. **Permitted Actions Without Identification or Authentication**  
*Authority - DIR CC: AC-14*

9.1 Component institutions must:

9.1.1 Identify and define user actions that can be performed on institutional information systems without identification or authentication consistent with institutional missions/business functions; and

9.1.2 Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

10. **Remote Access**  
*Authority - DIR CC: AC-17*

10.1 Component institutions must:

10.1.1 Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

10.1.2 Authorize remote access to each information system prior to allowing such connections.

11. **Wireless Access**  
*Authority - DIR CC: AC-18*

11.1 Component institutions must:

11.1.1 Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

11.1.2 Authorizes wireless access to the information system prior to allowing such connections.

12. **Access Control for Mobile Devices**  
*Authority - DIR CC: AC-19*

12.1 Component institutions must:

12.1.1 Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for institution-controlled mobile devices; and

12.1.2 Authorize the connection of mobile devices to institutional information systems.

13. **Use of External Information Systems**  
*Authority - DIR CC: AC-20*

13.1 Component institutions must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external
information systems, allowing authorized individuals to:

13.1.1 Access the information system from external information systems; and

13.1.2 Process, store, or transmit institution-controlled information using external information systems.

14. Publicly Accessible Content
Authority- DIR CC: AC-22

14.1 Component institutions must:

14.1.1 Designate individuals authorized to post information onto a publicly accessible information systems;

14.1.2 Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

14.1.3 Review, based on institution-defined criteria, the proposed content of information prior to posting onto publicly accessible information systems to ensure that nonpublic information is not included; and

14.1.4 Review, based on institution-defined criteria, the content on the publicly accessible information system for nonpublic information at institution-defined frequencies and removes such information, if discovered.
Awareness and Training Policy

Purpose: The purpose of this policy is to define information security controls around awareness and training.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Training implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Security Awareness and Training Policy

Authority - DIR Controls Catalog (CC): AT-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of security awareness and information security training;

3.1.2 Provide information security training for all users of university information systems; and

3.1.3 Review and update security awareness and training procedures at an institution-defined frequency.

4. Basic Security Awareness Training

Authority - DIR CC: AT-2, TGC 2054.5192

4.1 Component institutions must provide:

4.1.1 An ongoing information security awareness program to target all users;

4.1.2 Security awareness training for employees at least annually or as required by changes to information systems;

4.1.3 New employees with information security awareness training during the onboarding process; and
4.1.4 Security awareness training for contractors who have access to a component institution’s computer system or database.

5. **Role-Based Security Training**  
   Authority - DIR CC: AT-3

   5.1 Component institutions must provide role-based security training:

   5.1.1 To information resource employees with administrative privileges and responsibilities;

   5.1.2 Before authorizing access to information systems; and

   5.1.3 To information resource employees on a recurring basis (at least annually).

6. **Security Training Records**  
   Authority - DIR CC: AT-4

   6.1 Component institutions must:

   6.1.1 Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and

   6.1.2 Retain individual training records for an institution-defined time period.
Audit and Accountability Policy

Purpose: The purpose of this policy is to define information security controls around audit and accountability.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements
   1.1 Audit and accountability controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions
   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Audit and Accountability Policy
   Authority - DIR Controls Catalog (DIR CC): AU-1
   3.1 Component institutions must:
      3.1.1 Develop procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
      3.1.2 Review and update audit and accountability procedures at an institution-defined frequency.

4. Audit Events
   Authority - DIR CC: AU-2
   4.1 Component institutions must determine the capability of an information system for auditing institution-defined events.
   4.2 Component institution ISOs, or designee, shall coordinate with information system owners and custodians to help guide the selection of auditable security events.
   4.3 Component institutions must provide a rationale for why institution-defined auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
   4.4 Component institutions must determine:
4.4.1 What subset of events defined in 4.1 are to be audited within an information system; and,

4.4.2 The frequency at which events will be audited; or

4.4.3 Situations requiring auditing.

5. **Content of Audit Records**
   Authority - DIR CC: AU-3

5.1 Component institutions must ensure that information systems are configured to generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

6. **Audit Storage Capacity**
   Authority - DIR CC: AU-4

6.1 Component institutions must allocate audit record storage capacity in accordance with institution-defined audit record storage requirements.

7. **Response to Audit Processing Failures**
   Authority - DIR CC: AU-5

7.1 Information systems must be configured to alert appropriate information system custodians in the event of an audit processing failure.

8. **Audit Review, Analysis, and Reporting**
   Authority - DIR CC: AU-6

8.1 Component institutions must review and analyze information system audit records and report actionable findings to the appropriate information system custodians.

8.2 Review and analysis of information system audit records must occur at a frequency or in a manner determined by the component institution.

9. **Protection of Audit Information**
   Authority - DIR CC: AU-9

9.1 Component institutions must ensure that information systems protect audit information and audit tools from unauthorized access, modification, and deletion.

10. **Audit Record Retention**
    Authority - DIR CC: AU-11

10.1 Component institutions must retain audit records for a period no less than is required by its records retention policy and in order to provide sufficient support for after-the-fact investigations of security incidents.

11. **Audit Generation**
    Authority - DIR CC: AU-12

11.1 Component institutions must ensure that information systems:
11.1.1 Provide audit record generation capability for the auditable events defined in 4.1;

11.1.2 Allow information system custodians to select which auditable events are to be audited by specific components of the information system; and

11.1.3 Generate audit records for the events defined in 4.4.1 with the content defined in 5.1.
Security Assessment and Authorization Policy

Purpose: The purpose of this policy is to define information security controls around security assessment and authorization.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

   1.1 Security assessment and authorization controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Security Assessment and Authorization Policy

   Authority - DIR Controls Catalog (CC): CA-1

   3.1 Component institutions must:

      3.1.1 Develop procedures to facilitate the implementation of the Security Assessment and Authorization policy and associated assessment and authorization controls; and

      3.1.2 Review and update security assessment and authorization procedures at an institution-defined frequency.

4. Security Assessments

   Authority - DIR CC: CA-2

   4.1 Component institutions must:

      4.1.1 Develop a security assessment plan that describes the scope of the assessment including:

         4.1.1.1 Security controls and control enhancements under assessment;

         4.1.1.2 Assessment procedures to be used to determine security control effectiveness; and

         4.1.1.3 Assessment environment, assessment team, and assessment roles and respon-
4.1.2 Assess the security controls in the information system and its environment of operation on a recurring frequency established by the institution’s ISO to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

4.1.3 Produce a security assessment report that documents the results of the assessment; and

4.1.4 Provide the results of the security control assessment to appropriate personnel including information owners and custodians.

5. System Interconnections
Authority - DIR CC: CA-3

5.1 Component institutions must:

5.1.1 Through relevant information system owners, authorize interconnections between institutional information systems and other information systems, including those external to the institution;

5.1.2 Use a formalized Interconnection Security Agreement to document interconnections. At minimum, Interconnection Security Agreements must include the following information:

5.1.2.1 Interface characteristics;

5.1.2.2 Security requirements; and

5.1.2.3 The nature of the information communicated.

5.1.3 Regularly review and update as necessary established Interconnection Security Agreements at the time of periodic risk assessments or at an institution-defined frequency.

6. Plan of Action and Milestones
Authority - DIR CC: CA-5

6.1 Component institutions must:

6.1.1 Develop a Plan of Action and Milestones for each information system to document the institution’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls relevant to an information system and to reduce or eliminate known vulnerabilities in the assessed system; and

6.1.2 Update existing plans of action and milestones at an institution-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

7. Security Authorization
Authority - DIR CC: CA-6

7.1 Component institutions must:

7.1.1 Assign a senior-level executive or manager as the Authorizing Official for each information system;

7.1.2 Ensure that the Authorizing Official for an information system authorizes the information
system for processing before commencing operations; and

7.1.3 Update the security authorization at the time of periodic risk assessment for the information system or at an institution-defined frequency.

8. **Continuous Monitoring**
   Authority - DIR CC: CA-7

8.1 Component institutions must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

8.1.1 Establishment of metrics to be monitored;

8.1.2 Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;

8.1.3 Ongoing security control assessments in accordance with the institutional continuous monitoring strategy;

8.1.4 Ongoing security status monitoring of institution-defined metrics in accordance with the institutional continuous monitoring strategy;

8.1.5 Correlation and analysis of security-related information generated by assessments and monitoring;

8.1.6 Response actions to address results of the analysis of security-related information; and

8.1.7 Reporting the security status of the institution and the information system to appropriate stakeholders on institutionally defined frequency.

9. **Internal System Connections**
   Authority - DIR CC: CA-9

9.1 Each Component institution must:

9.1.1 Authorize internal connections of institution-defined information system components or classes of components to each information system; and

9.1.2 Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.
Configuration Management Policy

Purpose: The purpose of this policy is to define information security controls around configuration management.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Configuration management implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Configuration Management Policy

Authority - DIR Controls Catalog (CC): CM-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Configuration Management policy and associated configuration management controls; and

3.1.2 Review and update configuration management procedures at an institution-defined frequency.

4. Baseline Configuration

Authority - DIR CC: CM-2

4.1 Component institutions must develop, document, and maintain under configuration control, a current baseline configuration of the information system.

5. Security Impact Analysis

Authority - DIR CC: CM-4

5.1 Component institutions must analyze changes to information systems to determine potential security impacts prior to change implementation.

6. Configuration Settings

Authority - DIR CC: CM-6

6.1 Component institutions must:
6.1.1 Establish and document configuration settings for information technology products employed within the information system using institution-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

6.1.2 Implement the configuration settings;

6.1.3 Identify, document, and approve any deviations from established configuration settings for institution-defined information system components based on institution-defined operational requirements; and

6.1.4 Monitor and control changes to the configuration settings in accordance with institutional policies and procedures.

7. **Least Functionality**  
**Authority - DIR CC: CM- 7**

7.1 Component institutions must:

7.1.1 Configure each information system to provide only essential capabilities; and

7.1.2 Prohibit or restrict the use of institution-defined functions, ports, protocols, and/or services.

8. **Information System Component Inventory**  
**Authority - DIR CC: CM- 8**

8.1 Component institutions must:

8.1.1 Develop and document an inventory of information system components that:

8.1.1.1 Accurately reflects the current information system;

8.1.1.2 Includes all components within the Authorization Boundary of the information system;

8.1.1.3 Is at the level of granularity deemed necessary for tracking and reporting; and

8.1.1.4 Includes institution-defined information deemed necessary to achieve effective information system component accountability; and

8.1.2 Review and update the information system component inventory at an institution-defined frequency.

9. **Software Usage Restrictions**  
**Authority - DIR CC: CM- 10**

9.1 Component institutions must:

9.1.1 Use software and associated documentation in accordance with contract agreements and copyright laws;

9.1.2 Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

9.1.3 Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or...
10. User-Installed Software
Authority - DIR CC: CM-11

10.1 Component institutions must:

10.1.1 Establish institution-defined policies governing the installation of software by users;

10.1.2 Enforce software installation policies through institution-defined methods; and

10.1.3 Monitor policy compliance at institution-defined frequency.
Contingency Planning Policy

Purpose: The purpose of this policy is to define information security controls around contingency planning.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

   1.1 Contingency planning implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Contingency Planning Policy
   Authority - DIR Controls Catalog (CC): CP-1

   3.1 Component institutions must:
      3.1.1 Develop procedures to facilitate the implementation of the Contingency Planning policy and associated contingency planning controls; and
      3.1.2 Review and update contingency planning procedures at an institution-defined frequency.

4. Contingency Plan
   Authority - DIR CC: CP-2

   4.1 Component institutions must:
      4.1.1 Develop a contingency plan for each information system that:
         4.1.1.1 Identifies essential missions and business functions and associated contingency requirements;
         4.1.1.2 Provides recovery objectives, restoration priorities, and metrics;
         4.1.1.3 Addresses contingency roles, responsibilities, and assigned individuals with contact information;
4.1.1.4 Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

4.1.1.5 Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

4.1.1.6 Is reviewed and approved by institution-defined personnel or roles;

4.1.2 Distribute copies of the contingency plan to institution-defined key contingency personnel (identified by name and/or by role) and institutional elements;

4.1.3 Coordinate contingency planning activities with incident handling activities;

4.1.4 Review the contingency plan for the information system at an institution-defined frequency;

4.1.5 Update the contingency plan to address changes to the institution, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

4.1.6 Communicate contingency plan changes to institution-defined key contingency personnel (identified by name and/or by role) and institutional elements; and

4.1.7 Protect the contingency plan from unauthorized disclosure and modification.

5. **Contingency Training**
   Authority - DIR CC: CP-3

5.1 Component institutions must provide contingency training to information system users consistent with assigned roles and responsibilities:

5.1.1 Within an institution-defined time period of assuming a contingency role or responsibility;

5.1.2 When required by information system changes; and

5.1.3 On an institution-defined frequency thereafter.

6. **Contingency Testing**
   Authority - DIR CC: CP-4

6.1 Component institutions must:

6.1.1 Test the contingency plan for the information system on an institution-defined frequency using institution-defined tests to determine the effectiveness of the plan and the institutional readiness to execute the plan;

6.1.2 Review the contingency plan test results; and

6.1.3 Initiate corrective actions, if needed.

7. **Alternate Storage Site**
   Authority - DIR CC: CP-6

7.1 Component institutions must:

7.1.1 Establish an alternate storage site for Mission Critical information systems including
necessary agreements to permit the storage and retrieval of information system backup information; and

7.1.2 Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

8. **Information System Backup**  
   **Authority - DIR CC: CP-9**

   8.1 Component institutions must:

   8.1.1 Conduct backups of user-level information contained in the information system consistent with recovery time and recovery point objectives;

   8.1.2 Conduct backups of system-level information contained in the information system consistent with recovery time and recovery point objectives;

   8.1.3 Conduct backups of information system documentation including security-related documentation consistent with recovery time and recovery point objectives; and

   8.1.4 Protect the confidentiality, integrity, and availability of backup information at storage locations.

9. **Information System Recovery and Reconstitution**  
   **Authority - DIR CC: CP-10**

   9.1 Each component institution must have the capability for recovery and reconstitution of each information system to a known state after a disruption, compromise, or failure.
Identification and Authentication Policy

Purpose: The purpose of this policy is to define information security controls around identification and authentication.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Identification and authentication controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Identification and Authentication Policy

Authority - DIR Controls Catalog (CC): IA-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Identification and Authentication policy and associated identification and authentication controls; and

3.1.2 Review and update identification and authentication procedures at an institution-defined frequency.

4. Identification and Authentication

Authority - DIR CC: IA-2

4.1 Component institutions must ensure that information systems uniquely identify and authenticate institutional users (or processes acting on behalf of institutional users).

5. Identifier Management

Authority - DIR CC: IA-4

5.1 Component Institutions must manage information system identifiers by:

5.1.1 Receiving authorization from institution-defined personnel to assign an individual, group, role, or device identifier;
5.1.2 Selecting an identifier that identifies an individual, group, role, or device;

5.1.3 Assigning the identifier to the intended individual, group, role, or device;

5.1.4 Preventing reuse of identifiers for an organization-defined time period; and

5.1.5 Disabling the identifier after institution-defined time period of inactivity.

6. Authenticator Management
Authority - DIR CC: IA-5

6.1 Component Institutions must manage information system authenticators by:

6.1.1 Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

6.1.2 Establishing initial authenticator content for authenticators defined by the institution;

6.1.3 Ensuring that authenticators have sufficient strength of mechanism for their intended use;

6.1.4 Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

6.1.5 Changing default content of authenticators prior to information system installation;

6.1.6 Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

6.1.7 Changing/refreshing authenticators at an institution-defined time period by authenticator type;

6.1.8 Protecting authenticator content from unauthorized disclosure and modification;

6.1.9 Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

6.1.10 Changing authenticators for group/role accounts when membership to those accounts changes.

7. Authenticator Feedback
Authority - DIR CC: IA-6

7.1 Component institutions must ensure that information systems obscure feedback of authentication information entered during the authentication process.

8. Cryptographic Module Authentication
Authority - DIR CC: IA-7

8.1 Component institutions must follow all applicable laws and regulation regarding the use of cryptographic module authentication mechanisms for information systems.

9. Identification and Authentication (Non-Organizational Users)
Authority - DIR CC: IA-8
9.1 Component institutions must ensure that information systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).
Incident Response Policy

Purpose: The purpose of this policy is to define information security controls around incident response.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Incident response controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Incident Response Policy

Authority - DIR Controls Catalog (CC): IR-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Incident Response policy and associated incident response controls; and

3.1.2 Review and update incident response procedures at an institution-defined frequency.

4. Incident Response Training

Authority - DIR CC: IR-2

4.1 Component institutions must provide incident response training to information system users consistent with their assigned roles and responsibilities:

4.1.1 Within an institution-defined time period of assuming an incident response role or responsibility;

4.1.2 When required by information system changes; and

4.1.3 At an institution-defined frequency thereafter.

5. Incident Handling

Authority - Texas Administrative Code (TAC): 202.73(b); DIR CC: IR-4

5.1 Component institutions must:
5.1.1 Implement and maintain an incident handling capability to include preparation, detection and analysis, containment, eradication, recovery and coordination of incident handling activities with contingency planning activities;

5.1.2 Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

5.1.3 Assess the significance of information security incidents based on the business impact on the affected resources and the current potential technical effect of the incident.

6. Incident Monitoring
   Authority - TAC 202.73; DIR CC: IR-5

   6.1 Component institutions must track and document information system security incidents.

7. Incident Reporting
   Authority - TAC 202.73; DIR CC: IR-6

   7.1 Component institutions must:

   7.1.1 Require personnel to report suspected security incidents to the component institution’s Information Security Officer (ISO) or authorized designee using institution-defined procedures;

   7.1.2 Develop policies and mechanisms providing for notification to the designated ISO of any Suspected Data Breach within 48 hours of discovery;

   7.1.3 Promptly report security incidents to the Department of Information Resources (DIR) when the security incident is assessed to:

      7.1.3.1 Propagate to other state Information Systems;

      7.1.3.2 Result in criminal violations that shall be reported to law enforcement in accordance with state or federal information security or privacy laws; or

      7.1.3.3 Involve the unauthorized disclosure or modification of confidential information.

   7.1.4 Report summary security incident information monthly to DIR no later than 9 calendar days after the end of the month; and

   7.1.5 Establish reporting procedures which include a requirement that all personnel report suspected incidents to the ISO within a timeframe and method determined by the institution.

   7.2 If an information security incident is required to be reported to the DIR under Texas Government Code Sec. 2054.1125 or the “Urgent Incident Report” rules per Texas Administrative Code 202.73(b), the established event reporting and escalation procedures shall also require notification to the Texas State University System Administration via the Vice Chancellor and Chief Financial Officer and the Chief Audit Executive in a similar reporting manner and timeline.

8. Incident Response Assistance
   Authority - DIR CC: IR-7

   8.1 As an element of incident response capabilities, component institutions must provide incident response resources that advise and assist users of information resources in handling and reporting
security incidents.

8.2 Incident response resources are determined by each component institution’s Information Security Officer and may be comprised of technical support personnel, verified third-party consultants, and other resources.

9. **Incident Response Plan**  
**Authority - DIR CC: IR-8**

9.1 Component institutions must:

9.1.1 Develop an incident response plan that:

9.1.1.1 Provides the institution with a roadmap for implementing its incident response capability;

9.1.1.2 Describes the structure and organization of the incident response capability;

9.1.1.3 Provides a high-level approach for how the incident response capability fits in to the overall institution;

9.1.1.4 Meets the unique requirements of the institution, which relate to mission, size, structure, and functions;

9.1.1.5 Defines reportable incidents;

9.1.1.6 Provides metrics for measuring the incident response capability within the institution;

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

9.1.1.8 Is reviewed and approved by appropriate, institution-defined leadership.

9.1.2 Distribute copies of the incident response plan to appropriate personnel in an institution-defined manner;

9.1.3 Review and update the incident response plan as changes or problems are encountered or at least once annually, whichever occurs first;

9.1.4 Communicate changes to the incident response plan to appropriate personnel in an institution-defined manner; and

9.1.5 Protect the incident response plan from unauthorized disclosure and modification.
Maintenance Policy

Purpose: The purpose of this policy is to define information security controls regarding maintenance.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Maintenance controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. System Maintenance Policy and Procedures

Authority - DIR Controls Catalog (CC): MA-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the maintenance policy and associated maintenance controls; and

3.1.2 Review and update maintenance procedures at an institution-defined frequency.

4. Controlled Maintenance

Authority - DIR CC: MA-2

4.1 Information system custodians are responsible for scheduling, performing, documenting, and reviewing records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or component institution requirements.

4.2 Information system custodians are responsible for approving and monitoring all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

4.3 Component institutions must require that information system owners or custodians explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

4.4 Information system owners and custodians must ensure that equipment is sanitized to remove all information from associated media prior to removal from organizational facilities for off-site
4.5 Information system owners and custodians must check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

4.6 Information system owners and custodians must update appropriate organizational maintenance records following maintenance or repair actions.

5. **Nonlocal Maintenance**
   **Authority - DIR CC: MA-4**

5.1 Component institutions must:

   5.1.1 Approve and monitor nonlocal maintenance and diagnostic activities;

   5.1.2 Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

   5.1.3 Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

   5.1.4 Maintain records for nonlocal maintenance and diagnostic activities; and

   5.1.5 Terminate session and network connections when nonlocal maintenance is completed.

6. **Maintenance Personnel**
   **Authority - DIR CC: MA-5**

6.1 Component institutions must:

   6.1.1 Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

   6.1.2 Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations; and

   6.1.3 Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
Media Protection Policy

Purpose: The purpose of this policy is to define information security controls around media protection.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Media protection controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Security Awareness and Training Policy

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the media protection policy and associated media protection controls.

3.1.2 Review and update media protection procedures at an institution-defined frequency.

4. Media Access

4.1 Each component institution must develop procedures to restrict access to information system media.

4.2 Procedures must include, at minimum:

4.2.1 Definition of the types of media; and

4.2.2 Authorized personnel or roles.

5. Media Sanitization

5.1 Component institutions must:
5.1.1 Develop procedures to sanitize media prior to disposal, release out of organizational control, or release for reuse; and

5.1.2 Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the system.

6. **Media Use**
   
   Authority - DIR CC: MP-7

6.1 Each component institution shall develop procedures, standards, and safeguards governing the suitability of various types of media for institutional use.

6.2 Institutional procedures, standards, and safeguards must:

   6.2.1 Be based on the risk presented by the information system and the classification of data; and

   6.2.2 Designate which types of media are prohibited or restricted for institution-defined uses and information systems.
Network Management Policy

Purpose: The institutional network is a state information resource that exists to achieve the mission, goals, and objectives of Texas State University System and each component institution. Utilization of the network must be consistent with and in support of institutional initiatives. TAC 202 stipulates that access to state information resources must be appropriately managed.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Network Management controls by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1.2 The Texas State University System and its component institutions must ensure the confidentiality, integrity, and availability of their data, voice, and video networks to fulfill their institutional missions and to assure compliance with the management and security standards for public institutions of higher education described in TAC 202.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Network Management Policy

Authority - TSUS Board of Regents

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Network Management policy and associated network management controls; and

3.1.2 Review and update network management procedures at an institution-defined frequency.

4. Roles and Responsibilities

Authority - TSUS Board of Regents

4.1 Component institutions must:

4.1.1 Define a management framework which clearly delineates the roles and responsibilities for management of the institutional network;
4.1.2 Ensure the administration of the institutional network by the Information Resource Manager (IRM) or designee.

4.1.3 Ensure users and administrators of network-connected devices understand their accountability for device management and network usage practices that might result in damage or harm to network operations, performance, or other network-connected devices.

5. **Network Address and Device Management**  
   **Authority - TSUS Board of Regents**

5.1 Component institutions must ensure:

   5.1.1 The planning and coordination for the orderly assignment of network addresses; and

   5.1.2 The planning and coordination for the correct configuration of devices attached to the network.

5.2 Component institutions must ensure that all devices acting in the role of network infrastructure:

   5.2.1 Have a designated device administrator; and

   5.2.2 Are registered in a network device registry administered by the Information Resource Manager (IRM) or designee.

5.3 Component institutions must ensure that all devices acting in the role of a server (regardless of their specific function, hardware, software, or location):

   5.3.1 Have a designated device administrator; and

   5.3.2 Are registered in a network device registry administered by the Information Resource Manager (IRM) or designee.

6. **Threat and Incident Response**  
   **Authority – TSUS Board of Regents**

6.1 Component institutions must ensure:

   6.1.1 Network devices or addresses that pose an immediate threat to network operations, performance, or other network-connected devices are disconnected or quarantined to minimize risk until the threat is permanently removed; and

   6.1.2 Incident response actions comply with established, policy-defined controls and best practices regarding the preservation and treatment of forensic data.
Physical and Environmental Protection Policy

Purpose: The purpose of this policy is to define information security controls around physical and environmental protection.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 Physical and environmental protection controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1.2 Physical and environmental protection controls found in this policy apply to facilities under the custodianship of component institutions that house information systems.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Physical and Environmental Protection Policy

   Authority - DIR Controls Catalog (CC): PE-1

3.1 Component institutions must:

   3.1.1 Develop procedures to facilitate the implementation of the Physical and Environmental Protection policy and associated physical and environmental controls; and

   3.1.2 Review and update physical and environmental protection procedures at an institution-defined frequency.

4. Physical Access Authorizations

   Authority - DIR CC: PE-2

4.1 Component institutions must:

   4.1.1 Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides;

   4.1.2 Issue authorization credentials for facility access;

   4.1.3 Review the access list detailing authorized facility access by individuals at an
institution-defined frequency; and

4.1.4 Remove individuals from the facility access list when access is no longer required.

5. **Physical Access Control**  
**Authority - DIR CC: PE-3**

5.1 Component institutions must:

5.1.1 Enforce physical access authorizations at institution-defined entry and exit points to the facility where the information system resides by:

5.1.1.1 Verifying individual access authorizations before granting access to the facility; and

5.1.1.2 Controlling ingress to the facility using institution-defined physical access control systems;

5.1.2 Maintain physical access audit logs for institution-defined entry and exit points;

5.1.3 Provide institution-defined security safeguards to control access to areas within the facility officially designated as publicly accessible;

5.1.4 Escort visitors and monitor visitor activity based on institution-defined requirements;

5.1.5 Secure keys, combinations, and other physical access devices;

5.1.6 Inventories institution-defined physical access devices on an institution-defined frequency; and

5.1.7 Change combinations and keys on an institution-defined frequency and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

6. **Monitoring Physical Access**  
**Authority - DIR CC: PE-6**

6.1 Component institutions must:

6.1.1 Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents;

6.1.2 Review physical access logs on an institution-defined frequency and upon occurrence of institution-defined events or potential indications of events; and

6.1.3 Coordinate results of reviews and investigations with the institutional incident response capability.

7. **Visitor Access Records**  
**Authority - DIR CC: PE-8**

7.1 Component institutions must:

7.1.1 Maintain visitor access records to the facility where the information system resides for an institution-defined period; and

7.1.2 Review visitor access records on an institution-defined frequency.
8. **Emergency Lighting**  
Authority - DIR CC: PE-12

8.1 Component institutions must employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

9. **Fire Protection**  
Authority - DIR CC: PE-13

9.1 Component institutions must employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

10. **Temperature and Humidity Controls**  
Authority - DIR CC: PE-14

10.1 Component institutions must:

10.1.1 Maintain temperature and humidity levels within the facility where the information system resides at institution-defined acceptable levels; and

10.1.2 Monitor temperature and humidity levels at an institution-defined frequency.

11. **Water Damage Protection**  
Authority - DIR CC: PE-15

11.1 Component institutions must protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

12. **Delivery and Removal**  
Authority - DIR CC: PE-16

12.1 Component institutions must authorize, monitor, and control institution-defined types of information system components entering and exiting the facility and maintain records of those items.
Security Planning Policy

**Purpose:** The purpose of this policy is to define information security controls around security planning.

**Scope:** This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

**Application:** The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

**Review:** This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

**POLICY/PROCEDURE**

1. **Policy Statements**
   1.1 Security planning procedures implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. **Definitions**
   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. **Security Planning Policy**
   **Authority - DIR Controls Catalog (CC): PL-1**
   3.1 Component institutions must:
      3.1.1 Develop procedures to facilitate the implementation of security planning policy and associated security planning controls; and
      3.1.2 Review and update security planning procedures at an institution-defined frequency.

4. **System Security Plan**
   **Authority - DIR CC: PL-2**
   4.1 Each Information System under the custodianship of a component institution must have a corresponding System Security Plan that:
      4.1.1 Is consistent with the university’s enterprise architecture;
      4.1.2 Describes the function and security posture of the information system;
      4.1.3 Provides the security categorization of the information system, including supporting rationale;
      4.1.4 Describes the operational environment for the information system and relationships with or connections to other information systems;
      4.1.5 Provides an overview of the security requirements for the system that identifies the
security controls in place;

4.1.6 Identifies any relevant institution-defined overlays, if applicable; and

4.1.7 Is reviewed and approved by the information owner prior to plan implementation.

4.2 Copies of the System Security Plan and subsequent changes to the plan must be distributed to relevant stakeholders.

4.3 Component institutions must review and update System Security Plans on a recurring basis. This review must occur at an institution-defined frequency or when changes to the Information System or System Security Plan require it.

4.4 System Security Plans must be protected from unauthorized disclosure and modification.

5. Rules of Behavior
   Authority - DIR CC: PL-4

5.1 Each component institution must:

   5.1.1 Establish and make available to users an acceptable use policy for institutional information resources;

   5.1.2 Periodically update the institutional acceptable use policy; and

   5.1.3 Require its institutional users to acknowledge the acceptable use policy before authorizing access to information resources.

6. Content of Rules of Behavior
   Authority – TSUS Board of Regents

6.1 Each component institution’s rules of behavior must address, at minimum, the guidelines established in this section.

6.2 Institutional vs. Individual Purpose

   6.2.1 Users accessing institutional information resources are responsible for ensuring that their use of these resources is primarily for institutional purposes and institution-related activities.

   6.2.2 Access to information resources carries with it the responsibility for maintaining the security of the institution’s information resources.

   6.2.3 Rules for incidental use of institutional information resources.

   6.2.4 Individuals with authorized access to information resources must ensure that their access permissions are not accessible to or usable by any other individuals.

6.3 Personal vs. Official Representation

   6.3.1 Students, faculty, and staff using information resources to reflect the ideas, comments, and opinions of individual members of the institutional community must be distinguished from those that represent the official positions, programs, and activities of the institution.

   6.3.2 Students, faculty, and staff using information resources for purposes of exchanging,
publishing, or circulating official institutional documents must follow institutional requirements concerning appropriate content and style.

6.3.3 The institution is not responsible for the personal ideas, comments, and opinions of individual members of the institutional community expressed through the use of institutional information resources.

6.4 Limitations on the Availability of Information Resources

6.4.1 The institution’s information resources are finite by nature. All members of the institutional community must recognize that certain uses of institutional information resources may be limited or regulated as required to fulfill the institution’s primary teaching, research, and public service missions. Examples of these limitations include those related to capacity management, performance optimization, or security of the institution’s information systems.

6.5 Privacy and Confidentiality of Electronic Documents

6.5.1 No information system can absolutely guarantee the privacy or confidentiality of electronic documents.

6.5.2 Information resources provided by the TSUS and its component institutions are essentially owned by the State of Texas and subject to state oversight. Consequently, persons have no right to privacy in their use of institutional information resources even when using a personal or third-party device to access such resources.

6.5.3 TSUS institutions should take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons using institutional information resources that the institution will not seek access to their electronic messages or documents without their prior consent except where necessary to:

6.5.3.1 Satisfy the requirements of the Texas Public Information Act, or other statutes, laws, or regulations;

6.5.3.2 Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;

6.5.3.3 Protect the integrity of the institution’s information resources, and the rights and other property of the institution;

6.5.3.4 Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations; or

6.5.3.5 Protect the rights of individuals working in collaborative situations where information and files are shared.

6.5.4 TSUS institutions should establish procedures for appropriately preserving the privacy of electronic documents and for determining the methodology by which non-consensual access to electronic documents will be pursued by the institution.

6.6 Failure to Comply with Information Technology Policies

6.6.1 Failure to adhere to the provisions of TSUS IT policies or the IT policies of any component institution may result in:

6.6.1.1 Suspension or loss of access to institutional information resources;
6.6.1.2 Appropriate disciplinary action under existing procedures applicable to institutional users; and

6.6.1.3 Civil or criminal prosecution

6.6.2 To preserve and protect the integrity of information resources, there may be circumstances where the institution must immediately suspend or deny access to the resources. Should an individual’s access be suspended under these circumstances, the institution shall strive to inform the individual in a timely manner and afford the individual an opportunity to respond. The institution shall then determine what disciplinary action is warranted and shall follow the procedures established for such cases.
Program Management Policy

Purpose: The purpose of this policy is to define information security controls around program management.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements
   1.1 Program management controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions
   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Program Management Policy
   Authority - DIR Controls Catalog (CC): PM-1
   3.1 Component institutions must:
      3.1.1 Develop procedures to facilitate the implementation of the Program Management policy and associated program management controls; and
      3.1.2 Review and update program management procedures at an institution-defined frequency.

4. Senior Information Security Officer
   Authority - DIR CC: PM-2, Texas Administrative Code (TAC) 202.71, TAC 202.74
   4.1 Each component institution must appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an institution-wide information security program approved by the institution of higher education head or delegate.

5. Information Security Resources
   Authority - DIR CC: PM-3
   5.1 Component institutions must:
      5.1.1 Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this
5.1.2 Employ a business case or institution-defined documentation to record the resources required; and

5.1.3 Ensure that information security resources are available for expenditure as planned.

6. Plan of Action and Milestone Process
   Authority - DIR CC: PM-4

6.1 Component institutions must:

6.1.1 Implement a process for ensuring that plans of action and milestones for the security program and associated institutional information systems:

6.1.1.1 Are developed and maintained;

6.1.1.2 Document the remedial information security actions to adequately respond to risk to institutional operations and assets, individuals, and other organizations; and

6.1.1.3 Are reported in accordance with institution-defined reporting requirements.

6.1.2 Review plans of action and milestones for consistency with the institutional risk management strategy and institution-wide priorities for risk response actions.

7. Information System Inventory
   Authority - DIR CC: PM-5

7.1 Component institutions must develop and maintain an inventory of their information systems.

8. Information Security Measures of Performance
   Authority - DIR CC: PM-6

8.1 Component institutions must develop, monitor, and report to institution-defined individuals on the results of information security measures of performance.

9. Enterprise Architecture
   Authority - DIR CC: PM-7

9.1 Component institutions must develop an enterprise architecture with consideration for information security and the resulting risk to institutional operations, institutional assets, individuals, and other organizations.

10. Threat Awareness Program
    Authority - DIR CC: PM-16

10.1 Component institutions must implement a threat awareness program that includes a cross-organization information-sharing capability.
Personnel Security Policy

Purpose: The purpose of this policy is to define information security controls around personnel security.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements
   1.1 Personnel security controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions
   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Personnel Security Policy
   Authority - DIR Controls Catalog (CC): PS-1
   3.1 Component institutions must:
      3.1.1 Develop procedures to facilitate the implementation of the Personnel Security policy and associated personnel security controls; and
      3.1.2 Review and update personnel security procedures at an institution-defined frequency.

4. Position Risk Designation
   Authority - DIR CC: PS-2
   4.1 Each component institution must:
      4.1.1 Assign a risk designation to all institutional positions;
      4.1.2 Establish screening criteria for individuals filling those positions; and
      4.1.3 Review and update position risk designations at an institution-defined frequency.

5. Personnel Screening
   Authority - DIR CC: PS-3
   5.1 Each component institution must:
      5.1.1 Screen individuals prior to authorizing access to information systems; and
5.1.2 Rescreen individuals when institution-defined conditions require rescreening.

6. Personnel Termination
Authority - DIR CC: PS-4

6.1 Each component institution, upon termination of an individual’s employment, must:

6.1.1 Disable information system access and terminate/revoke any authenticators/credentials associated with the individual within an institution-defined time period;

6.1.2 Conduct exit interviews that include a discussion of institution-defined information security topics that include review of any signed non-disclosure agreements and secure disposition of university data from personal devices in a manner stipulated by the institution;

6.1.3 Retrieve all security-related, institutional information system-related property;

6.1.4 Retain access to institutional information and information systems formerly controlled by terminated individual; and

6.1.5 Notify institution-defined personnel within an institution-defined time period.

7. Personnel Transfer
Authority - DIR CC: PS-5

7.1 Each component institution must:

7.1.1 Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the institution;

7.1.2 Initiate transfer or reassignment actions within an institution-defined time period following the formal transfer action;

7.1.3 Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and

7.1.4 Notify institution-defined personnel within an institution-defined time period.

8. Access Agreements
Authority - DIR CC: PS-6

8.1 Each component institution must:

8.1.1 Develop and document access agreements for institutional information systems;

8.1.2 Review and update the access agreements at an institution-defined frequency; and

8.1.3 Ensure that individuals requiring access to institutional information and information systems:

8.1.3.1 Sign appropriate access agreements prior to being granted access; and

8.1.3.2 Re-sign access agreements to maintain access to institutional information systems when access agreements have been updated or at an institution-defined frequency.
9. **Third-Party Personnel Security**  
**Authority - DIR CC: PS-7**

9.1 Each component institution must:

9.1.1 Establish personnel security requirements including security roles and responsibilities for third-party providers;

9.1.2 Require third-party providers to comply with personnel security policies and procedures established by the institution;

9.1.3 Document personnel security requirements;

9.1.4 Require third-party providers to notify institution-defined personnel of any personnel transfers or terminations of third-party personnel who possess institutional credentials and/or badges, or who have information system privileges within an institution-defined time period; and

9.1.5 Monitors provider compliance.

10. **Personnel Sanctions**  
**Authority - DIR CC: PS-8**

10.1 Each component institution must:

10.1.1 Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

10.1.2 Notify institution-defined personnel within institution-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
Risk Assessment Policy

Purpose: The purpose of this policy is to define information security controls around risk assessment.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

   1.1 Risk assessment controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Risk Assessment Policy

   Authority - DIR Controls Catalog (CC): RA-1

   3.1 Component institutions must:

      3.1.1 Develop procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

      3.1.2 Review and update risk assessment procedures at an institution-defined frequency.

4. Security Categorization

   Authority - DIR CC: RA-2, TAC 202.75

   4.1 Each component institution ISO must establish requirements for security categorization of information systems.

   4.2 Component institutions must:

      4.2.1 Categorize information and information systems, at a minimum of “high”, “moderate”, or “low”, and in accordance with applicable laws, regulations and policies;

      4.2.2 Document the security categorization results, including supporting rationale, in the information system security plan; and

      4.2.3 Ensure that the security categorization decision is reviewed and approved by information system owner.
5. **Risk Assessment**  
Authority - DIR CC: RA-3, TAC 202

5.1 Component institutions must:

5.1.1 Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

5.1.2 Review and document risk assessment results in a report on a recurring frequency determined by the institution's ISO;

5.1.3 Disseminate risk assessment results to the Institutional ISO;

5.1.4 Perform risk assessments on information systems on a recurring frequency determined by the institution or when significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system occur; and

5.2 Authorization of security risk acceptance, transference, or mitigation decisions shall be the responsibility of:

5.2.1 The ISO or their designee(s), in coordination with the information owner, for systems identified with low or moderate residual risk; or

5.2.2 The component institution's President for all systems identified with a residual high risk.

6. **Vulnerability Scanning**  
Authority - DIR CC: RA-5

6.1 Component Institutions must:

6.1.1 Scan for vulnerabilities in each information system and its hosted applications on a recurring frequency, at least annually, in accordance with each component institution’s established process and when new vulnerabilities potentially affecting systems or applications are identified and reported;

6.1.2 Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards defined by each component institution’s ISO for:

6.1.2.1 Enumerating platforms, software flaws, and improper configurations;

6.1.2.2 Formatting checklists and test procedures; and

6.1.2.3 Measuring vulnerability impact;

6.1.3 Analyze vulnerability scan reports and results from security control assessments;

6.1.4 Remediate legitimate vulnerabilities in accordance with an organizational assessment of risk; and

6.1.5 Share information obtained from the vulnerability scanning process and security control assessments with appropriate information system custodians in accordance with component institution's internal dissemination procedures.
1. Risk Assessment
   Authority - DIR CC: RA-3, TAC 202

   1.1 Component institutions must:

      1.1.1 Conduct an assessment of risk, including the likelihood and magnitude of harm, from
            the unauthorized access, use, disclosure, disruption, modification, or destruction of the
            information system and the information it processes, stores, or transmits;

      1.1.2 Review and document risk assessment results in a report on a recurring frequency
            determined by the institution's ISO;

      1.1.3 Disseminate risk assessment results to the Institutional ISO;

      1.1.4 Perform risk assessments on information systems on a recurring frequency determined
            by the institution or when significant changes to the information system or environment
            of operation, or other conditions that may impact the security state of the system occur;
            and

   1.2 Authorization of security risk acceptance, transference, or mitigation decisions shall be the
   responsibility of:

      1.2.1 The ISO or their designee(s), in coordination with the information owner, for systems
            identified with low or moderate residual risk; or

      1.2.2 The component institution's President for all systems identified with a residual high risk.

2. Vulnerability Scanning
   Authority - DIR CC: RA-5

   2.1 Component Institutions must:

      2.1.1 Scan for vulnerabilities in each information system and its hosted applications on a
            recurring frequency, at least annually, in accordance with each component institution’s
            established process and when new vulnerabilities potentially affecting systems or
            applications are identified and reported;

      2.1.2 Employ vulnerability scanning tools and techniques that facilitate interoperability among
            tools and automate parts of the vulnerability management process by using standards
            defined by each component institution’s ISO for:

            2.1.2.1 Enumerating platforms, software flaws, and improper configurations;

            2.1.2.2 Formatting checklists and test procedures; and

            2.1.2.3 Measuring vulnerability impact;

      2.1.3 Analyze vulnerability scan reports and results from security control assessments;

      2.1.4 Remediate legitimate vulnerabilities in accordance with an organizational assessment of
            risk; and

      2.1.5 Share information obtained from the vulnerability scanning process and security control
            assessments with appropriate information system custodians in accordance with
            component institution's internal dissemination procedures.
System and Services Acquisition Policy

Purpose: The purpose of this policy is to define information security controls around system and services acquisition.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

   1.1 System and services acquisition controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. System and Services Acquisition Policy

   Authority - DIR Controls Catalog (CC): SA-1

   3.1 Component institutions must:

       3.1.1 Develop procedures to facilitate the implementation of the System and Services Acquisition policy and associated system and services acquisition controls; and

       3.1.2 Review and update system and services acquisition procedures at an institution-defined frequency.

4. Allocation of Resources

   Authority - DIR CC: SA-2

5. Component institutions must:

   5.1 Determine information security requirements for each information system or information system service in mission/business process planning;

   5.2 Determine, document, and allocate the resources required to protect each information system or information system service as part of its capital planning and investment control process; and

   5.3 Establish a discrete line item for information security in institutional programming and budgeting documentation.
6. **System Development Life Cycle**
Authority - DIR CC: SA-3

6.1 Component institutions must:

6.1.1 Manage the information system using an institution-defined system development life cycle that incorporates information security considerations;

6.1.2 Define and document information security roles and responsibilities throughout the system development life cycle;

6.1.3 Identify individuals having information security roles and responsibilities; and

6.1.4 Integrate the institutional information security risk management process into system development life cycle activities.

7. **Acquisition Process**
Authority - DIR CC: SA-4

7.1 Component institutions must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for each information system, system component, or information system service in accordance with applicable federal/state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and institutional mission/business needs:

7.1.1 Security functional requirements;

7.1.2 Security strength requirements;

7.1.3 Security assurance requirements;

7.1.4 Security-related documentation requirements;

7.1.5 Requirements for protecting security-related documentation;

7.1.6 Description of the information system development environment and environment in which the system is intended to operate; and

7.1.7 Acceptance criteria.

8. **Information System Documentation**
Authority - DIR CC: SA-5

8.1 Each component institution must:

8.1.1 Obtain administrator documentation for each information system, system component, or information system service that describes:

8.1.1.1 Secure configuration, installation, and operation of the system, component, or service;

8.1.1.2 Effective use and maintenance of security functions/mechanisms; and

8.1.1.3 Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

8.1.2 Obtain user documentation for each information system, system component, or
information system service that describes:

8.1.2.1 User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

8.1.2.2 Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

8.1.2.3 User responsibilities in maintaining the security of the system, component, or service;

8.1.3 Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and take institution-defined actions in response;

8.1.4 Protect documentation as required, in accordance with the risk management strategy; and

8.1.5 Distribute documentation to institution-defined personnel.

9. External Information System Services
Authority - DIR CC: SA-9

9.1 Component institutions must:

9.1.1 Require that providers of external information system services comply with institutional information security requirements and employ institution-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

9.1.2 Define and document government oversight and user roles and responsibilities with regard to external information system services; and

9.1.3 Employ institution-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

10. Developer Configuration Management
Authority - DIR CC: SA-10

10.1 Component institutions must require the developer of each information system, system component, or information system service to:

10.1.1 Perform configuration management during system, component, or service during at least one of the following stages: design, development, implementation, operation;

10.1.2 Document, manage, and control the integrity of changes to institution-defined configuration items under configuration management;

10.1.3 Implement only institution-approved changes to the system, component, or service;

10.1.4 Document approved changes to the system, component, or service and the potential security impacts of such changes; and

10.1.5 Track security flaws and flaw resolution within the system, component, or service and report findings to institution-defined personnel.
System and Communications Protection

Purpose: The purpose of this policy is to define information security controls around system and communications protection.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 System and communications protection controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. System and Communications Protection Policy

Authority - DIR Controls Catalog (CC): SC-1

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the System and Communications Protection policy and associated system and communications protection controls; and

3.1.2 Review and update system and communications protection procedures at an institution-defined frequency.

4. Denial of Service Protection

Authority - DIR CC: SC-5

4.1 Component institutions must protect information systems against or limit the effects of institutionally identified denial of service attacks by employing institutionally defined safeguards.

5. Boundary Protection

Authority - DIR CC: SC-7

5.1 Each information system must:

5.1.1 Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; and
5.1.2 Implement subnetworks for publicly accessible system components that are either physically or logically separated from internal organizational networks; and

5.1.3 Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

6. **Transmission Confidentiality and Integrity**
   Authority - DIR CC: SC-8

   6.1 Each information system must protect the confidentiality and/or integrity of transmitted information.

7. **Cryptographic Key Establishment and Management**
   Authority - DIR CC: SC-12

   7.1 Component institutions must establish and manage cryptographic keys for required cryptography employed within each information system in accordance with institutionally defined requirements for key generation, distribution, storage, access, and destruction.

8. **Cryptographic Protection**
   Authority - DIR CC: SC-13

   8.1 Each information system must implement institutionally defined cryptographic uses and type of cryptography required for each use in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

9. **Collaborative Computing Devices**
   Authority - DIR CC: SC-15

   9.1 Each information system must:

   9.1.1 Prohibit remote activation of collaborative computing devices except for devices specifically defined by the institution; and

   9.1.2 Provide an explicit indication of use to users physically present at the devices.

10. **Secure Name / Address Resolution Service (Authoritative Source)**
    Authority - DIR CC: SC-20

    10.1 Each information system that provides name resolution services must:

    10.1.1 Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

    10.1.2 Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

11. **Secure Name / Address Resolution Service (Recursive or Caching Resolver)**
    Authority - DIR CC: SC-21

    11.1 Each information system that provides recursive name resolution or name caching must request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
12. **Architecture and Provisioning for Name / Address Resolution Service**  
*Authority - DIR CC: SC-22*

12.1 Each information system that collectively provides name/address resolution service for an institution are fault-tolerant and implement internal/external role separation.

13. **Process Isolation**  
*Authority - DIR CC: SC-39*

13.1 Each information system must maintain a separate execution domain for each executing process.
Server Management Policy

Purpose: Institutional servers are state information resource that exist to achieve the mission, goals, and objectives of Texas State University System and each component institution. Utilization of these servers must be consistent with and in support of institutional initiatives. TAC 202 stipulates that access to state information resources must be appropriately managed.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

   1.1 Server Management controls by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

   1.2 The Texas State University System and its component institutions must ensure the confidentiality, integrity, and availability of their server hardware and software to fulfill their institutional missions and to assure compliance with the management and security standards for public institutions of higher education described in TAC 202.

2. Definitions

   2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. Server Management Policy

   Authority - TSUS Board of Regents

   3.1 Component institutions must:

      3.1.1 Develop procedures to facilitate the implementation of the Server Management policy and associated server management controls; and

      3.1.2 Review and update server management procedures at an institution-defined frequency.

4. Roles and Responsibilities

   Authority - TSUS Board of Regents

   4.1 Component institutions must define a management framework which clearly delineates the roles and responsibilities for management of servers.

   4.2 The framework must delineate distinct roles for a server owner and a server administrator that:
4.2.1 Establish the responsibilities of server owners to include:

4.2.1.1 Establishment of server usage requirements;

4.2.1.2 Specification of server access controls (both physical and electronic);

4.2.1.3 Assurance of compliance with state and institutional server management standards; and

4.2.1.4 Designation of a separate primary and secondary server administrator.

4.2.2 Establish the responsibilities of server administrators to include:

4.2.2.1 Enforcement of the owner's usage requirements;

4.2.2.2 Implementation of the owner-specified access controls; and

4.2.2.3 Configuration of the server according to the required standards.

5. Server Management Standards
   Authority - TSUS Board of Regents

5.1 Component institutions must:

5.1.1 Develop, document, and make available a server management standard in alignment with established, policy-defined controls, and best practices;

5.1.2 Develop, document, make available, and implement compliance review procedures; and

5.1.3 Ensure that all exceptions to this requirement are documented and justified through risk management decisions.

6. Threat and Incident Response
   Authority - TSUS Board of Regents

6.1 Component institutions must ensure:

6.1.1 Servers that pose an immediate threat to network operations, performance, or other network-connected devices are disconnected or quarantined to minimize risk until the threat is permanently removed; and

6.1.2 Incident response actions comply with established, policy-defined controls and best practices regarding the preservation and treatment of forensic data.
System and Information Integrity Policy

Purpose: The purpose of this policy is to define information security controls around system and information integrity.

Scope: This policy applies to the Texas State University System and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution’s information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Review: This policy will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

POLICY/PROCEDURE

1. Policy Statements

1.1 System and information controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

3. System and Information Integrity Policy

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the System and Information Integrity policy and associated system and information integrity controls; and

3.1.2 Review and update system and information integrity procedures at an institution-defined frequency.

4. Flaw Remediation

4.1 Component institutions must:

4.1.1 Identify, report, and correct information system flaws;

4.1.2 To the extent practicable, test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

4.1.3 Install security-relevant software and firmware updates within an institution-defined time period of the release of the updates; and

4.1.4 Incorporate flaw remediation into the institutional configuration management process.
5. **Malicious Code Protection**  
   Authority - DIR CC: SI-3

5.1 Component institutions must:

5.1.1 Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

5.1.2 Update malicious code protection mechanisms whenever new releases are available in accordance with institutional configuration management policy and procedures;

5.1.3 Configure malicious code protection mechanisms to:

   5.1.3.1 Perform periodic scans of the information system at an institution-defined frequency and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with institutional security policy; and

   5.1.3.2 Perform one or more of the following in response to malicious code detection: block malicious code; quarantine malicious code; send alert to administrator; or perform another institution-defined action; and

5.1.4 Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

6. **Information System Monitoring**  
   Authority - DIR CC: SI-4

6.1 Component institutions must:

6.1.1 Monitor each information system to detect:

   6.1.1.1 Attacks and indicators of potential attacks in accordance with institution-defined monitoring objectives; and

   6.1.1.2 Unauthorized local, network, and remote connections;

6.1.2 Identify unauthorized use of the information system through institution-defined techniques and methods;

6.1.3 Deploy monitoring devices:

   6.1.3.1 Strategically within the information system to collect institutional-determined essential information; and

   6.1.3.2 At ad hoc locations within the system to track specific types of transactions of interest to the institution;

6.1.4 Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

6.1.5 Heighten the level of information system monitoring activity whenever there is an indication of increased risk to institutional operations and assets, individuals, or other organizations on law enforcement information, intelligence information, or other credible sources of information;
6.1.6 Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

6.1.7 Provide institution-defined information system monitoring information to institution-defined personnel as needed and/or at an institution-defined frequency.

7. **Security Alerts, Advisories, and Directives**  
   **Authority - DIR CC: SI-5**

7.1 Component institutions must:

7.1.1 Receive information system security alerts, advisories, and directives from institution-defined external organizations on an ongoing basis;

7.1.2 Generate internal security alerts, advisories, and directives as deemed necessary;

7.1.3 Disseminates security alerts, advisories, and directives to institution-defined personnel and/or institution-defined external organizations; and

7.1.4 Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

8. **Information Handling and Retention**  
   **Authority - DIR CC: SI-12**

8.1 Component institutions must handle and retain information within each information system and information output from each system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
TSUS Information Technology Glossary

Purpose: A glossary of Information Technology terms used in TSUS and Component institutions’ policies and other information technology documents.

Scope: The glossary terms are considered to have the same meaning at each component.

Application: Components may supplement the TSUS Information Technology Glossary with additional terms and definitions used in their documents but may not alter the meaning or definition of the existing terms.

Review: This glossary will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

GLOSSARY

Access - The physical or logical capability to view, interact with, or otherwise make use of Information Resources.

Acceptable Risk - The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific information system.

Access Control - The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., data centers, physical plant, mechanical rooms, Network closets, secured buildings, and research laboratories).

Acquisition - Includes all stages of the process of acquiring products or services, beginning with the process for determining the need for the product or service and ending with contract completion and closeout.

Administrative Privileges - Rights granted to a Privileged User.

Attribute - A claim of a named quality or characteristic inherent in or ascribed to someone or something.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational Procedures.

Audit Log / Audit Records - A chronological record of Information System activities, including records of system Accesses and operations performed in a given period.

Auditable Event - Events which are significant and relevant to the security of Information Systems and the environments in which those systems operate in order to meet specific and ongoing Audit needs. Audit events can include, for example, Password changes, failed logons, or failed accesses related to Information Systems, Administrative Privilege usage, or third-party credential usage.

Authentication - Verifying the Identity of a User, process, or Device, often as a prerequisite to allowing Access to resources in an Information System.
Authenticator - The means used to confirm the Identity of a User, process, or Device (e.g., User Password or token).

Authorization - The right or a permission that is granted to a system entity to access a system resource.

Authorization Boundary - All components of an Information System to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the Information System is connected.

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating an Information System at a level of Acceptable Risk to institution operations (including mission, functions, image, or reputation), institution assets, or individuals.

Availability - The security objective of ensuring timely and reliable Access to and use of information.

Best Practice - See Guideline.

Business Function - Process or operation performed routinely to carry out a part of the mission of an institution.

Business Impact Analysis (BIA) - An analysis of an Information System’s requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or Procedures that describe how the institution’s mission/business processes will be sustained during and after a significant disruption.

Certificate Authority - The entity in a Public Key Infrastructure (PKI) that is responsible for issuing public-key certificates and exacting compliance to a PKI policy. Also known as a Certification Authority.

Collaborative Computing Device - Tools that facilitate and enhance group work through distributed technology - where individuals collaborate from separate locations. Devices can include but are not limited to Networked white boards, cameras, and microphones.

Confidential Information - Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

Confidentiality - The security objective of preserving authorized restrictions on information Access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control - Process for controlling modifications to hardware, Firmware, software, and documentation to protect the Information System against improper modifications before, during, and after system implementation.

Configuration Management - A collection of activities focused on establishing and maintaining the Integrity of information technology products and Information Systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems.
Contingency Plan - Management policy and Procedures used to guide an institution response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the institutional Risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or disaster recovery plan (DRP) for major disruptions.

Continuity of Operations Plan (COOP) - See Business Continuity Plan.

Cryptographic - Relating to the discipline that embodies the principles, means, and methods for the transformation of Data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Cryptographic Module - Any combination of hardware, Firmware or software that implements Cryptographic functions such as Encryption, Decryption, Digital Signatures, Authentication techniques and random number generation.

Cryptographic Module Authentication - The set of hardware, software, Firmware, or some combination thereof that implements Cryptographic logic or processes, including Cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Custodian - See Information Custodian.

Data - Information in a specific representation, usually as a sequence of symbols that have meaning.

Decryption - The process of changing ciphertext into plaintext using a Cryptographic algorithm and key.

Device - Any hardware component involved with the processing, storage, or forwarding of information making use of the institutional information technology infrastructure or attached to the Institutional Network. These Devices include, but are not limited to, laptop computers, desktop computers, Servers, and Network Devices such as routers, switches, wireless access points, and printers.

Device Administrator - An individual with principal responsibility for the installation, configuration, registration, security, and ongoing maintenance of a Network-connected Device.

Device Owner - The department head charged with overall responsibility for the Networking component in the institution's inventory records. The Device Owner must designate an individual to serve as the primary Device Administrator and may designate a backup Device Administrator. All Network Infrastructure Devices, (e.g., Network cabling, routers, switches, wireless access points, and in general, any non-endpoint Device) shall be centrally owned and administered.

Digital Signature - The result of a Cryptographic transformation of Data which, when properly implemented, provides the services of: 1. origin Authentication, 2. Data Integrity, and 3. signer non-repudiation.

DIR CC – The security control catalog (CC) authored by the Texas Department of Information Resources (DIR) which provides state agencies and higher education institutions specific guidance for implementing security controls in a format that easily aligns with the National Institute of
Encryption - The conversion of plaintext information into a code or cipher text using a variable called a “key” and processing those items through a fixed algorithm to create the Encrypted text that conceals the Data’s original meaning.

Execution Domain - Each Information System process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

External Information System Service - An Information System service that is implemented outside of the Authorization Boundary of the institutional Information System (i.e., a service that is used by, but not a part of, the institutional Information System) and for which the institution typically has no direct control over the application of required security controls or the assessment of security control effectiveness. Examples include but are not limited to externally hosted or cloud-based Information Systems.

External Network - A Network not controlled by the institution.

Federal Information Processing Standards (FIPS) - A Standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Firewall - An inter-Network connection Device that restricts Data communication traffic between two connected Networks. A Firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a Network. Typically, Firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Firmware - Computer programs and Data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and Data cannot be dynamically written or modified during execution of the programs.

Guideline - Guidelines provide guidance for achieving additional positive outcomes. Guidelines are not compulsory unless explicitly stated, but they should still be followed when practicable. Guidelines can also be used as prescriptive or informational documents.

Identification - The process of discovering the true Identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identifier - Unique Data used to represent a person’s Identity and associated Attributes. A name or a card number are examples of Identifiers. Note: This also encompasses non-person entities.

Identity - The set of Attributes by which an entity is recognizable and that, within the scope of an Identity manager’s responsibility, is sufficient to distinguish that entity from any other entity.

Incident Response - The mitigation of violations of security policies and Best Practices.
**Information Custodian** - A department, agency, or Third Party Provider responsible for implementing the Information Owner-defined controls and Access to an Information Resource.

**Information Owner** - A person(s) with statutory or operational authority for specified information or Information Resources.

**Information Resource Employee** - Agency employees performing administrative, security, governance, or compliance activities on information technology systems. These types of employees generally have an occupational Category of “Information Technology” per the Texas State Auditor's Office or similar duties.

**Information Resources** - the Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors. Information Resources include but are not limited to:

- all physical and logical components, wired or wireless, of the Institutional Network;
- any Device that connects to or communicates electronically via the Institutional Network, including computers, printers, and communication Devices, both portable and fixed;
- any fixed or portable storage Device or media, regardless of ownership, that contains institution Data;
- all Data created, collected, recorded, processed, stored, retrieved, displayed, or transmitted using Devices connected to the Institutional Network;
- all computer software and services licensed by the institution;
- support staff and services employed or contracted by the institution to deploy, administer, or operate the above-described resources or to assist the community in effectively using these resources;
- Devices, software, or services that support the operations of the institution, regardless of physical location (e.g., SAAS, PAAS, IAAS, cloud services); and
- telephones, audio and video conferencing systems, phone lines, and communications systems provided by the institution.

**Information Resources Management (IRM)** - The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by institutions.

**Information Security** - The protection of information and Information Systems from Unauthorized Access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, Integrity, and Availability.

**Information Security Officer (ISO)** - The individual designated by the institution head who has the explicit authority and the duty to administer Information Security requirements institution wide.

**Information System** - An interconnected set of Information Resources that share a common functionality. An Information System normally includes, but is not limited to, hardware, software, Network Infrastructure, information, applications, communications and people.

**Information System Entry and Exit Points** - These include but are not limited to Firewalls, electronic mail Servers, web Servers, proxy Servers, Remote Access Servers, workstations, notebook computers, and mobile Devices.
**Information System Components** - All components of an Information System to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the Information System is connected.

**Information System Owner** - See Information Custodian.

**Institutional Elements** - Organizations, departments, facilities, or personnel responsible for a particular system's process.

**Institutional Network** - The Data transport and communications infrastructure at the institution. It includes the campus backbone, local area networks, and all equipment connected to those Networks (independent of ownership).

**Integrity** - The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

**Interconnection Security Agreement** - A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection.

**Internet** - The single, interconnected, worldwide system of commercial, governmental, educational, and other computer Networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

**Intranet** - A computer Network, especially one based on Internet technology, that the institution uses for its own internal (and usually private) purposes and that is closed to outsiders.

**Least Privilege** - The principle that a security architecture should be designed so that each entity is granted the minimum system resources and Authorizations that the entity needs to perform its function.

**Malicious Code** - Rogue computer programs designed to inflict a magnitude of harm by diminishing the Confidentiality, Integrity and Availability of Information Systems and information.

**Malware** - Software or Firmware intended to perform an unauthorized process that will have adverse impact on the Confidentiality, Integrity, or Availability of an Information System. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of Malware.

**Management Controls** - The security controls (i.e., safeguards or countermeasures) for an Information System that focus on Risk Management and the management of Information System security.

**Managed Interfaces** - An interface within an Information System that provides boundary protection capability using automated mechanisms or Devices.
**Metrics** - Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related Data.

**Mission Critical** - Information Resources defined by the owner or by the institution to be crucial to the continued performance of the mission. Unavailability of such Information Resources would result in more than an inconvenience. An event causing the unavailability of Mission Critical Information Resources would result in consequences such as: significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations.

**Network** - Information System(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control Devices.

**Network Address** - A unique number associated with a Device’s Network connection used for the routing of traffic across the Internet or another Network. Also known as Internet Protocol Address or IP Address.

**Network Infrastructure** - The hardware and software resources of an entire Network that enable Network connectivity, communication, operations and management of an enterprise Network. It provides the communication path and services between Users, processes, applications, services and External Networks/the Internet. These include but are not limited to cabling, routers, switches, hubs, Firewall appliances, wireless access points, virtual private network (VPN) Servers, network address translators (NAT), proxy Servers, and dial-up Servers.

**NIST** - National Institute of Standards and Technology.

**Node** - A Device or object connected to a Network.

**Non-organizational User** - A User who is not an institutional User (including public Users).

**Organizational Users** - An institutional User that the institution deems to have an affiliation including, for example, faculty, staff, student, contractor, guest researcher, or individual detailed from another organization.

**Password** - A type of Authenticator comprised of a string of characters (letters, numbers, and other symbols) used to authenticate an Identity or to verify Authorization.

**Penetration Testing** - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

**Personally Identifiable Information (PII)** - A category of personal Identity information as defined by §521.002(a)(1), Business and Commerce Code.

**Plan of Action and Milestone (POA&M)** - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

**Private Key** - A Cryptographic key, used with a Cryptographic algorithm, that is uniquely associated with an entity and is not made public.
Privileged Account - An Information System account with approved Authorizations of a Privileged User.

Privileged User - A User that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary Users are not authorized to perform.

Procedure - An operational-level document that details actions needed to implement a security control, configure a solution, or complete a task. Some Procedures may be compulsory, and other Procedures may just be one way of doing something. Procedures specify “how” things need to be done.

Protected Health Information (PHI) - Individually identifiable health information about an individual, including demographic information, which relates to the individual's past, present, or future physical or mental health condition, provision of health care, or payment for the provision of health care.

Public Key - A cryptographic key used with a cryptographic algorithm that is uniquely associated with an entity and that may be made public.

Public Key Certificate - A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it.

Reconstitution - Returning Information Systems to fully operational states.

Recovery Point Objective (RPO) - The point in time to which Data must be recovered after an outage.

Recovery Time Objective (RTO) - The overall length of time an Information System's components can be in the recovery phase before negatively impacting the institution’s mission or mission/business processes.

Remote Access - Access to an institutional Information System by a User (or an Information System) communicating through an External Network (e.g., the Internet).

Residual Risk - Portion of Risk remaining after security measures have been applied.

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Assessment - The process of identifying Risks to institutional operations (including mission, functions, image, reputation), institutional assets, individuals, other institutions, resulting from the operation of a system. Part of Risk Management, incorporates threat and Vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with Risk analysis.

Risk Management - The total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes Risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security
review.

**Risk Tolerance** - The degree of Risk or uncertainty that is acceptable to an institution.

**Role-Based Access Control (RBAC)** - Access Control based on User roles (i.e., a collection of Authorizations a User receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an institution. A given role may apply to a single individual or to several individuals.

**Security Assessment** - The testing and/or evaluation of the management, operational, and technical security controls in an Information System to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

**Security Control Assessments** - See Security Assessment.

**Security Categorization** - The characterization of information or an Information System as high, moderate, or low based on an assessment of the potential impact that a loss of Confidentiality, Integrity, or Availability of such information or Information System would have on institutional operations, institutional assets, or individuals.

**Security Classification** - The categorization of information based on its need for Confidentiality, as determined by federal, state, local laws, policies or regulations.

**Sensitive Personal Information (SPI)** - A category of personal Identity information as defined by §521.002(a)(2), Texas Business and Commerce Code.

**Separation of Duty** - A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or Access privilege to perpetrate damaging fraud.

**Server** - A physical or virtual Device that performs a specific service or function on behalf of other Network Devices or Users.

**Server Administrator** - A type of Information Custodian designated by the Server Owner as responsible for performing Server Management functions.

**Server Management** - Functions associated with the oversight of Server operations. These include controlling User Access, establishing/maintaining security measures, monitoring Server configuration and performance, and Risk Assessment and mitigation.

**Server Owner** - An institution employee charged with overall responsibility for the Server asset in the university’s inventory records.

**Standard** - A tactical-level, compulsory requirement to use the same technology, method, security control, baseline, or course of action to uniformly achieve the goals set by policies. Standards specify “what” needs to be done.

**Suspected Data Breach** - Is any incident in which sensitive, confidential or otherwise protected
Data in human or machine-readable form is put at Risk because of exposure to unauthorized individuals.

**System Level Information** - Information that includes but is not limited to, system-state information, operating system and application software, and licenses.

**System Security Plan (SSP)** - Formal document that provides an overview of the security requirements for an Information System and describes the security controls in place or planned for meeting those requirements.

**Third Party Providers** - Service providers, staffing, integrators, vendors, telecommunications, and infrastructure support that are external to the institution.

**Unauthorized Access** - A person gains logical or physical Access without permission to institutional Information Resources.

**User** - An individual, process, or automated application authorized to access an Information Resource in accordance with federal and state law, institution policy, and the Information Owner's Procedures and rules.

**User Level Information** - Any information other than System Level Information.

**Vulnerability** - Weakness in an Information System, system security Procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Vulnerability Assessment** - Systematic examination of an Information System or product to determine the adequacy of security measures, identify security deficiencies, provide Data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.