THE TEXAS STATE UNIVERSITY SYSTEM®

System IT Policies

November 2022

Glossary

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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;

3.1.2 Review and update Access Control procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Access Control procedures related to the controls in this policy.

4. **Account Management & Disable Accounts**

Authority - DIR CC: AC-2, AC-2(3) TAC 202.72

4.1 Component institutions must:

4.1.1 Define 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 and conditions;

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

4.1.8 Notify account managers (i.e., information owners) within an institution-defined period of time for each of the following conditions:

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 information system usage or need-to-know changes for an individual;

4.1.9 Require that determinations to authorize access to each information system by the respective information owner are 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 least once every two years or more frequently as defined by the component institution;

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

4.1.12 Align account management processes with personnel termination and transfer processes; and

4.1.13 Disable accounts within an institution-defined period of time when the accounts:

4.1.13.1 Have expired;

4.1.13.2 Are no longer associated with a user or individual;

4.1.13.3 Are in violation of institutional policy; or

4.1.13.4 Have been inactive for an institution-defined period of time.

5. Access 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 Identify and document separation of duties of individuals based on institution-defined criteria; and

6.1.2 Require that information owners define information system access authorizations to support separation of duties.

7. Least Privilege

Authority – DIR CC: AC-6

7.1 Component institutions must:

7.1.1 Establish the principle of least privilege as a critical and strategic component of institution-level information security policies and procedures; and

7.1.2 Ensure that access to information systems for users and processes acting on behalf of users is based on the principle of least privilege.

8. Unsuccessful Logon Attempts

Authority - DIR CC: AC-7

8.1 Component institutions must ensure that each information system:

8.1.1 Enforces an institution-defined limit of consecutive, invalid logon attempts by a user or source of authentication during an institution-defined period of time; and

8.1.2 Automatically performs at least one of the following actions when the maximum number of unsuccessful attempts is exceeded:

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

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

8.1.2.3 Delays the next logon prompt according to an institution-defined delay algorithm; and/or

8.1.2.4 Notifies the information custodian.

9. System Use Notification

Authority - DIR CC: AC-8

9.1 Component institutions must ensure that each information system:

9.1.1 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:

9.1.1.1 Users are accessing an institutional information system;

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

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

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

9.1.2 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

9.1.3 For publicly accessible information systems that do not have logon interfaces:

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

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

9.1.3.3 Includes a description of the authorized uses of the system.

10. Permitted Actions Without Identification or Authentication

Authority - DIR CC: AC-14

10.1 Component institutions must:

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

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

11. Remote Access

Authority - DIR CC: AC-17

11.1 Component institutions must:

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

11.1.2 Authorize each type of remote access to each information system prior to allowing such connections.

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

12.1 Component institutions must:

12.1.1 Establish configuration and connection requirements, and implementation guidance for each type of wireless access; and

12.1.2 Authorize each type of wireless access to each information system prior to allowing such connections.

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

13.1 Component institutions must:

13.1.1 Establish configuration requirements, connection requirements, and implementation guidance for institution-controlled mobile devices, to include when such devices are outside of institutionally controlled networks; and

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

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

14.1 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:

14.1.1 Access the information system from external information systems; and

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

15. **Publicly Accessible Content**
Authority- DIR CC: AC-22

15.1 Component institutions must:

15.1.1 Designate individuals authorized to make information publicly accessible;

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

15.1.3 Review the proposed content of information prior to posting onto publicly accessible information systems to ensure that nonpublic information is not included; and

15.1.4 Review the content on the publicly accessible information system for nonpublic information at institution-defined frequencies and remove 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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

Authority - DIR Controls Catalog (CC): AT-1, TGC 2054.519, TGC 5054.5191, TGC 2054.5192

3.1 Component institutions must:

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

3.1.2 Review and update Awareness and Training procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Awareness and Training procedures related to the controls in this policy; and

3.1.4 Provide information security training for all users of institutional information systems in accordance with applicable state and federal law, including, but not limited to, Texas Government Code § 2054.519, §2054.5191, and §2054.5192;

4. **Awareness Training**
Authority - DIR CC: AT-2, TGC 2054.519, TGC 2054.5191, TGC 2054.5192

4.1 Component institutions must:

4.1.1 Provide security awareness training to:

4.1.1.1 Employees at least annually or as required by changes to information systems;

4.1.1.2 New employees during the onboarding process; and

4.1.1.3 Contractors who have access to a component institution's computer system or database.

4.1.2 Update security awareness training at an institution-defined frequency.

5. **Role-Based Training**
Authority - DIR CC: AT-3, TGC 2054.519, TGC 2054.5191, TGC 2054.5192

5.1 Component institutions must:

5.1.1 Provide role-based security training:

5.1.1.1 To information resource employees with administrative privileges and responsibilities;

5.1.1.2 Before authorizing access to information systems, information, or performing assigned duties;

5.1.1.3 To information resource employees on a recurring basis (at least annually) and when required by system changes.

5.1.2 Update role-based training content at an institution-defined frequency.

6. **Training Records**
Authority - DIR CC: AT-4, TGC 2054.519, TGC 2054.5191, TGC 2054.5192

6.1 Component institutions must:

6.1.1 Document and monitor information security training activities, including security awareness training and specific role-based 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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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 controls;

3.1.2 Review and update Audit and Accountability procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Audit and Accountability procedures related to the controls in this policy.

4. **Event Logging**

Authority - DIR CC: AU-2

4.1 Component institutions must:

4.1.1 Document a standard defining the types of events that each information system shall log, including the frequency at which the types of events selected for logging are reviewed and updated;

4.1.2 Identify, for each information system, the types of events that the system is capable of logging in support of the audit function as specified in the component institution's Standard;

4.1.3 Require information owners and information custodians to coordinate with each component institution's ISO (or their designee) to coordinate event logging functions;

4.1.4 Specify the types of events from its standard that are configured for logging within each information system along with the frequency of (or situation requiring) logging for each identified type of event;

4.1.5 Provide a rationale for why institution-defined auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

4.1.6 Review and update event types selected for logging according to the Standard for each information system.

4.2 Component institutions must:

4.2.1 Ensure information systems provide the means whereby authorized personnel have the ability to audit and establish individual accountability for each action that can potentially cause access to, generation or modification of, or affect the release of confidential information;

4.2.2 Ensure appropriate audit trails are maintained to provide accountability for updates to mission-critical information, hardware and software, and for all changes to automated security or access rules; and

4.2.3 Based upon an assessment of risk, maintain a sufficiently complete history of transactions to permit an audit of the information system by logging and tracing the activities of individuals through each information system.

5. Content of Audit Records

Authority - DIR CC: AU-3

5.1 Component institutions must ensure that each information system's audit records contain the following information:

5.1.1 What type of event occurred;

5.1.2 When the event occurred;

5.1.3 Where the event occurred;

5.1.4 Source of the event;

5.1.5 Outcome of the event; and

5.1.6 Identity of any individuals, subjects, or objects/entities associated with the event.

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

6.1 Component institutions must:

6.1.1 Allocate audit-log storage capacity to accommodate institution-defined audit log retention requirements.

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

7.1 Component institution must:

7.1.1 Document in a standard the audit processing failures that generate alerts, the appropriate personnel or roles to alert, the time period in which to be alerted, and any additional actions to take;

7.1.2 In accordance with the standard, configure information systems to send designated alerts to appropriate personnel or roles in the event of applicable audit processing failures; and

7.1.3 Take any additional actions in accordance with the standard in the event of an audit logging process failure of an information system.

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

8.1 Component institutions must:

8.1.1 Document in a standard the frequency at which information system audit records are reviewed and analyzed;

8.1.2 Review and analyze information system audit records in accordance with the frequency specified in the standard and report actionable findings to the appropriate information system custodians; and

8.1.3 Adjust the level of audit record review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

9. **Time Stamps**
Authority - DIR CC: AU-8

9.1 Component institutions must:

9.1.1 Configure each information system to:

9.1.1.1 Use internal system clocks to generate time stamps for audit records; and

9.1.1.2 Synchronize internal system clocks with an authoritative source of time specified by the component institution;

9.1.2 Ensure that audit records record time stamps in milliseconds and:

9.1.2.1 Use Coordinated Universal Time;

9.1.2.2 Have a fixed local time offset from Coordinated Universal Time; or

9.1.2.3 Include the local time offset as part of the timestamp.

10. Protection of Audit Information

Authority - DIR CC: AU-9

10.1 Component institutions must protect audit information and audit tools from unauthorized access, modification, and deletion.

11. Audit Record Retention

Authority - DIR CC: AU-11

11.1 Component institutions must:

11.1.1 Ensure records retention policies for audit records meets regulatory and institutional information retention requirements; and

11.1.2 Retain audit records for a period no less than is required by its records retention policy to provide sufficient support for after-the-fact investigations of security incidents.

12. Audit Record Generation

Authority - DIR CC: AU-12

12.1 Component institutions must ensure that information systems:

12.1.1 Provide audit record generation capability for the auditable events required by this policy and related institutional policies and standards;

12.1.2 Allow authorized personnel or roles to select which auditable events are to be audited by specific components of the information system; and

12.1.3 In alignment with this policy and related institutional policies and standards, generate audit records for necessary types of events and ensure the generated records contain sufficient content.

Assessment, Authorization, and Monitoring Policy

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

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

POLICY/PROCEDURE

1. **Policy Statements**

1.1 Security Assessment, Authorization, and Monitoring 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. **Procedures**

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, Authorization, and Monitoring policy and associated controls;

3.1.2 Review and update Security Assessment, Authorization, and Monitoring procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Assessment, Authorization, and Monitoring procedures related to the controls in this policy.

4. **Control Assessments**

Authority - DIR CC: CA-2

4.1 Component institutions must:

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

4.1.1.1 Controls and control enhancements under assessment;

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

4.1.1.3 Assessment environment, assessment team, and assessment roles and responsibilities;

4.1.2 Ensure the control assessment plan is reviewed and approved by the authorizing official or the authorizing official's designated representative prior to conducting the assessment;

4.1.3 Assess the 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;

4.1.4 Produce a control assessment report that documents the results of the assessment; and

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

4.2 Component institutions must ensure that a review of the institution's information security program for compliance with security standards set by the Texas Department of Information Resources is performed at least biennially, based on institutional risk management decisions. The review must be performed by individual(s) independent of the institution's information security program and designated by the institution's head or their designated representative(s).

5. Information Exchange

Authority - DIR CC: CA-3

5.1 Component institutions must:

5.1.1 Through relevant information system owners, authorize the exchange of information (i.e., 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 for each information system:

5.1.2.1 Interface characteristics;

5.1.2.2 Security requirements, controls, and responsibilities;

5.1.2.3 Information system category; and

5.1.2.4 The nature of the information communicated, including data classification.

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 controls assessments, audits, and continuous monitoring activities.

7. 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 Assign a senior-level executive or manager as the Authorizing Official for common controls available for inheritance by institutional information systems;

7.1.3 Ensure that the Authorizing Official for an information system accepts the use of common controls inherited by the system and authorizes the information system for processing before commencing operations;

7.1.4 Ensure that the Authorizing Official for common controls authorizes the use of those controls for inheritance by institutional information systems; and

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

8. Continuous Monitoring & Risk Monitoring

Authority - DIR CC: CA-7, CA-7(4)

8.1 Component institutions must develop a continuous monitoring strategy and implement an information system-level continuous monitoring program that includes:

8.1.1 Establishment of system-level metrics to be monitored;

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

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

8.1.4 Ongoing monitoring of information system and institution-defined metrics in accordance with the institutional continuous monitoring strategy;

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

8.1.6 Response actions to address results of the analysis of control assessment and monitoring information; and

8.1.7 Reporting the security status of each information system to appropriate stakeholders at an institutional-defined frequency.

8.2 Component institutions must ensure that risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

8.2.1 Effectiveness monitoring;

8.2.2 Compliance monitoring; and

8.2.3 Change monitoring.

9. Penetration Testing

Authority - DIR CC: CA-8; TGS §2054.516(a)(2)

9.1 Each component institution must conduct penetration testing at an institution-defined frequency on institution-defined information systems and information system components.

9.2 Component institutions must ensure that:

9.2.1 Internet websites or mobile applications that process any sensitive personal information, personally identifiable information, or confidential information are subjected to a vulnerability and penetration test at an institution-defined frequency; and

9.2.2 Ensure that any vulnerability identified in each test is addressed in a fashion commensurate to the risks presented as determined by the institution's ISO (or designee).

10. Internal System Connections

Authority - DIR CC: CA-9

10.1 Each component institution must:

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

10.1.2 Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated;

10.1.3 Terminate internal system connections based on institution-defined conditions; and

10.1.4 Review the need for each internal connection at an institution-defined frequency.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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 controls;

3.1.2 Review and update Configuration Management procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Configuration Management procedures related to the controls in this policy.

4. **Baseline Configuration**

Authority - DIR CC: CM-2

4.1 Component institutions must:

4.1.1 Develop, document, and maintain under configuration control, a current baseline configuration of each information system; and

4.1.2 Review and update the baseline configuration of each information system:

4.1.2.1 At an institution-defined frequency;

4.1.2.2 When required because of institution-defined circumstances; and

4.1.2.3 When information system components are installed or upgraded.

5. **Impact Analyses**
Authority - DIR CC: CM- 4

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

5.2 Component institutions must ensure that:

5.2.1 All security-related information resources changes are approved by the information owner (or designee) through a change control process; and

5.2.2 Such approval occurs prior to implementation by the institution or independent contractors.

6. **Access Restrictions for Change**
1. Authority - DIR CC: CM- 5

6.1 Component institutions must define, document, approve, and enforce physical and logical access restrictions associated with changes to each information system.

7. **Configuration Settings**
Authority - DIR CC: CM- 6

7.1 Component institutions must:

7.1.1 Establish and document configuration settings for components employed within information systems using institution-defined, common security configurations that reflect the most restrictive mode consistent with operational requirements;

7.1.2 Implement the configuration settings;

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

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

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

8.1 Component institutions must:

8.1.1 Configure each information system to provide only institution-defined, mission-essential capabilities; and

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

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

9.1 Component institutions must:

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

9.1.1.1 Accurately reflects the information system;

9.1.1.2 Includes all components within each information system;

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

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

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

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

10.1 Component institutions must:

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

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

10.1.3 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 reproduction of copyrighted work.

11. **User-Installed Software**
Authority - DIR CC: CM- 11

11.1 Component institutions must:

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

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

11.1.3 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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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 controls;

3.1.2 Review and update Contingency Planning procedures at an institution-defined frequency;

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Contingency Planning procedures related to the controls in this policy; and

3.1.4 Maintain written continuity of operations plans that address information resources.

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 controls 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 each 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 Plan Testing**
Authority - DIR CC: CP-4

6.1 Component institutions must:

6.1.1 Test the contingency plan for information systems at least annually 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, 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 controls equivalent to that of the primary site.

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

8.1 Component institutions must:

8.1.1 Conduct backups of the following types of information at a frequency consistent with institution-defined recovery time and recovery point objectives:

8.1.1.1 User-level information contained in information systems;

8.1.1.2 System-level information contained in information systems; and

8.1.1.3 Information system documentation, including security-related documentation;

8.1.2 Protect the confidentiality, integrity, and availability of backup information.

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

9.1 Component institutions must have the capability for recovery and reconstitution of each information system to a known state after a disruption, compromise, or failure consistent with institution-defined recovery time and recovery point objectives.

10. **Alternate Communications Protocols**
Authority - DIR CC: CP-11

10.1 Component institutions must have the capability to employ institution-defined alternative communications protocols in support of maintaining continuity of operations.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

    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 controls;

        3.1.2 Review and update Identification and Authentication procedures at an institution-defined frequency; and

        3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Identification and Authentication procedures related to the controls in this policy.

4. **Identification and Authentication (Organizational Users), Multifactor Authentication to Privileged Accounts, & Multifactor Authentication to Non-privileged Accounts**

Authority - DIR CC: IA-2, IA-2(1), IA-2(2); TAC 202.1

4.1 Component Institutions must ensure that information systems uniquely identify and authenticate institutional users or processes acting on behalf of institutional users prior to granting the user or process access to a given information system.

4.1.1 Non-unique identifiers may only be used in situations in which risk analysis performed by institution-defined personnel demonstrates no need for individual accountability of users.

4.2 Component Institutions must implement multifactor authentication for access to privileged accounts on institutional information systems.

4.3 Component Institutions must implement multifactor authentication for access to non-privileged accounts on institutional information systems.

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, service, or device identifier;

5.1.2 Selecting an identifier that identifies an individual, group, role, service, or device;

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

5.1.4 Preventing reuse of identifiers for an institution-defined time period.

5.2 Component Institutions must ensure a user's access authorization is appropriately modified or removed when the user's employment, job responsibilities, or affiliation with the institution changes.

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, service, 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 authenticators prior to first use;

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

6.1.7 Changing or 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 controls to protect authenticators; and

6.1.10 Changing authenticators for group or 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 authentication processes.

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

8.1 Component institutions must:

8.1.1 Implement mechanisms for authentication to cryptographic modules in information systems; and

8.1.2 Ensure that implemented cryptographic modules meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

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-institutional users or processes acting on behalf of non-institutional users.

10. **Re-Authentication**
Authority - DIR CC: IA-11

10.1 Component institutions must document a Standard defining the circumstances or situations which require users to re-authenticate.

10.2 Component institutions must require users to re-authenticate according to the component institution's Standard.

10.3 Component institutions' standard for re-authentication must include the following minimum requirements:

10.3.1 Users must be required to re-authenticate when a device automatically locks; and

10.3.2 Users must be required to re-authenticate when the user's password is known to be compromised or publicly disclosed.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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 controls; and

3.1.2 Review and update Incident Response procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Incident Response procedures related to the controls in this policy.

3.2 Each component institution must assess the significance of a security incident based upon the business impact on the affected resources and the current and potential technical effect of the incident.

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 or acquiring information system access;

4.1.2 When required by information system changes; and

4.1.3 At an annual frequency thereafter.

5. **Incident Response Testing**
Authority - DIR CC: IR-3

5.1 Component institutions must test the effectiveness of the incident response capability for each information system at an institution-defined frequency using the institution-defined tests for each information system.

6. **Incident Handling**
Authority - Texas Administrative Code (TAC): 202.73(b); DIR CC: IR-4

6.1 Component institutions must:

6.1.1 Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery

6.1.2 Coordinate incident handling activities with contingency planning activities;

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

6.1.4 Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the institution.

7. **Incident Monitoring**
Authority - TAC 202.73(b); DIR CC: IR-5

7.1 Component institutions must track and document security and supply chain incidents.

8. **Incident Reporting**
Authority - TAC 202.73(b); DIR CC: IR-6

8.1 Component institutions must:

8.1.1 Require personnel to report suspected security and supply chain incidents to the component institution's ISO (or their designee) using institution-defined procedures within an institution-defined time period;

8.1.2 Develop policies and mechanisms providing for notification to the ISO (or their designee) any Suspected Data Breach within 48 hours of discovery;

8.1.3 Promptly report security and supply chain incidents to the Department of Information Resources (DIR) when the security incident is assessed to:

8.1.3.1 Propagate to other state information systems;

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

8.1.3.3 Involve the unauthorized disclosure or modification of confidential information; or

8.1.3.4 be an unauthorized incident that compromises, destroys, or alters information systems, applications, or access to such systems or applications in any way.

8.1.4 Report summary security and supply chain incident information monthly to DIR no later than 9 calendar days after the end of the month.

8.2 If an information security or supply chain 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 component institution's established 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.

9. Incident Response Assistance

Authority - DIR CC: IR-7

9.1 Component institutions must provide an incident response resource, integral to the component institution's incident response capability, that advises and assists users of information systems in handling and reporting security and supply chain incidents. The incident response resource must be determined by each component institution's ISO and may be comprised of technical support personnel, verified third-party consultants, and other resources.

10. Incident Response Plan

Authority - DIR CC: IR-8

10.1 Component institutions must:

10.1.1 Develop an incident response plan that:

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

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

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

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

10.1.1.5 Defines reportable incidents;

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

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

10.1.1.8 Is reviewed and approved by appropriate, institution-defined leadership; and

10.1.1.9 Explicitly designates responsibility for incident response to institution-defined roles.

10.1.2 Distribute copies of the incident response plan to institutional elements charged with incident response responsibilities defined by name and/or role;

10.1.3 Update the incident response plan to address system and institutional changes or problems encountered during plan implementation, execution, or testing;

10.1.4 Communicate changes to the incident response plan to institutional elements charged with incident response responsibilities defined by name and/or role; and

10.1.5 Protect the incident response plan from unauthorized disclosure and modification.

11. Information Spillage Response

Authority - DIR CC: IR-9

11.1 Component institutions must respond to information spills by:

11.1.1 Assigning, in the incident response plan, personnel or roles with responsibility for responding to information spills;

11.1.2 Identifying the specific information involved in the information system contamination;

11.1.3 Alerting personnel identified in the incident response plan of the information spill using a method of communication not associated with the spill;

11.1.4 Isolating the contaminated information system or information system component;

11.1.5 Eradicating the information from the contaminated information system or component;

11.1.6 Identifying other information systems or information system components that may have been subsequently contaminated; and

11.1.7 Performing any additional actions defined in the incident response plan.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **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 controls;

3.1.2 Review and update Maintenance procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Maintenance procedures related to the controls in this policy.

4. **Controlled Maintenance**
Authority - DIR CC: MA-2

4.1 Component institutions must require information custodians to:

4.1.1 Schedule, document, and review records of maintenance, repair, and/or replacement on information system components in accordance with manufacturer or vendor specifications and/or institution-defined requirements;

4.1.2 Approve and monitor all maintenance activities, whether performed on site or remotely and whether the information system or information system components are serviced on site or removed to another location;

4.1.3 Explicitly approve the removal of the information system or information system components from institutional facilities for off-site maintenance, repair, and/or replacement;

4.1.4 Sanitize equipment to remove all information from associated media prior to removal from institutional facilities for off-site maintenance, repair, and/or replacement;

4.1.5 Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair, and/or replacement actions; and

4.1.6 Update appropriate institutional maintenance records following maintenance, repair, and/or replacement actions.

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

5.1 Component institutions, directly or contractually, 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 institutional 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 Verify that non-escorted personnel performing maintenance on information systems possess the required access authorizations; and

6.1.3 Designate institutional 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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. Procedures

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

3.1. Component institutions must:

3.1.1. Develop procedures to facilitate the implementation of the Media Protection policy and associated controls;

3.1.2. Review and update Media Protection procedures at an institution-defined frequency; and

3.1.3. Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Media Protection procedures related to the controls in this policy.

4. Media Access

Authority - DIR CC: MP-2

4.1. Component institutions must restrict access to institution-defined types of digital and non-digital media to institution-defined personnel or roles.

5. Media Sanitization

Authority - Texas Government Code (TGC) 441.185; DIR CC: MP-6

5.1. Component institutions must:

5.1.1. Sanitize institution-defined system media prior to disposal, release out of institutional control, or release for reuse using institution-defined sanitization techniques and procedures; and

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

5.2. Component institutions must:

5.2.1. Destroy electronic records in accordance with Texas Government Code § 441.185 and in compliance with the institution's records retention schedule;

5.2.2. Retain, for the duration of the required retention period, a hard copy or other electronic copy of records from data processing equipment at the time of removal if the applicable retention period for the record has not expired;

5.2.3. Consider the incorporation guidelines from the Texas Department of Information Resources regarding the sale or transfer of computers and software into institutional policies, standards, guidelines, and procedures; and

5.2.4. Keep a record or form, in electronic or hard copy, documenting the removal of records and/or system media and completion of associated processes, including, at minimum, the following information:

5.2.4.1. Date;

5.2.4.2. Description of the item(s) and serial number(s);

5.2.4.3. Inventory number(s);

5.2.4.4. The process and sanitization tools used to remove the data or method of destruction; and

5.2.4.5. The name and address of the organization to which the equipment was transferred.

6. Media Use

Authority - DIR CC: MP-7

6.1. Component institutions must document and enforce a Standard defining at minimum:

6.1.1. The types of system media within scope of the Standard;

6.1.2. Whether and under what conditions, including on what information systems or information system components, the use of each type of system media is authorized, restricted, or prohibited; and

6.1.3. Controls required to use authorized types of system media.

6.2. Each component institution must prohibit the use of portable storage devices in institutional systems when such devices have no identifiable owner.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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 controls;

3.1.2 Review and update Physical and Environmental Protection procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Physical and Environmental Protection procedures related to the controls in this policy.

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 facilities in which one or more institutional information systems reside;

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 facilities in which one or more institutional information systems reside by:

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

5.1.1.2 Controlling ingress and egress to each facility using institution-defined physical access control systems, which may include systems, devices, and/or guards;

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

5.1.3 Control access to areas within each facility designated as publicly accessible using institution-defined controls;

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 Inventory institution-defined physical access devices at an institution-defined frequency; and

5.1.7 Change combinations and keys:

5.1.7.1 At an institution-defined frequency; and/or

5.1.7.2 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 facilities in which one or more institutional information

systems reside to detect and respond to physical security incidents;

6.1.2 Review physical access logs at 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 facilities in which one or more institutional information systems reside for an institution-defined period;

7.1.2 Review visitor access records at an institution-defined frequency; and

7.1.3 Report anomalies in visitor access records to institution-defined personnel.

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 facilities in which one or more institutional information systems reside.

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

9.1 Component institutions must employ and maintain fire suppression and detection devices or systems for facilities in which one or more institutional information systems reside that are supported by an independent energy source.

10. **Environmental Controls**
Authority - DIR CC: PE-14

10.1 Component institutions must:

10.1.1 Maintain temperature and humidity levels within facilities in which one or more institutional information systems reside at institution-defined acceptable levels; and

10.1.2 Monitor environmental control levels at an institution-defined frequency.

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

11.1 Component institutions must protect facilities in which one or more institutional information systems reside 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:

12.1.1 Authorize and control institution-defined types of information system components entering and exiting facilities in which one or more institutional information systems reside; and

12.1.2 Maintain records of institution-defined information system components.

13. Alternate Work Site

Authority - DIR CC: PE-17

13.1 Component institutions must:

13.1.1 Determine and document institution-defined alternate work sites allowed for use by employees;

13.1.2 Employ institution-defined controls at alternate work sites;

13.1.3 Assess the effectiveness of controls at alternate work sites; and

13.1.4 Provide a means for employees to communicate with information security personnel in case of incidents.

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 requirement;

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.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

Authority - DIR Controls Catalog (CC): PL-1, TAC 202.73

3.1 Component institutions must:

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

3.1.2 Review and update Security Planning procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Security Planning procedures related to the controls in this policy.

3.2 Each component institution's information security officer must report annually on the institution's information security program to their respective institution head in compliance with 1 Texas Administrative Code §202.73(a).

4. System Security and Privacy Plans

Authority - DIR CC: PL-2

4.1 Component institutions must ensure that each information system under the institution's custodianship has a corresponding System Security Plan that:

4.1.1 Is consistent with the institution's enterprise architecture;

4.1.2 Explicitly defines the constituent information system component(s);

4.1.3 Describes the function and security posture of the information system, including in terms of mission and business processes;

4.1.4 Provides the security categorization of the information system and highest classification of information it stores, processes, and/or transmits, including supporting rationale;

4.1.5 Describes any specific threats to the information system that are of concern to the institution;

4.1.6 Describes the operational environment for the information system and relationships with or connections to other information systems;

4.1.7 Provides an overview of the security requirements for the information system that identifies the security controls in place;

4.1.8 Identifies any relevant security control baselines and, if applicable, institution-defined overlays;

4.1.9 Describes the controls in place or planned for meeting the security requirements, including a rationale for any tailoring decisions;

4.1.10 Includes risk determinations for security architecture and design decisions;

4.1.11 Includes in a plan of action and milestones security-related activities affecting the information system that require planning and coordination with institution-defined individuals or groups; and

4.1.12 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 Component institutions must:

5.1.1 Establish and provide to users (including, but not limited to, state agency personnel, temporary employees, and employees of independent contractors) an acceptable

use policy for institutional information resources that describes the users' responsibilities and expected behavior for the usage and security of information and Information Resources;

5.1.2 Periodically review and update the institutional acceptable use policy;

5.1.3 Require institutional users to acknowledge the acceptable use policy and indicate that the users have read, understand, and agree to abide by the acceptable use policy before authorizing access to the information and Information Resources; and

5.1.4 Require individuals who have acknowledged a previous version of the acceptable use policy to read and re-acknowledge when rules are revised or updated or at least annually as part of mandatory cybersecurity training.

6. Data Classification, Security, and Retention Requirements for Information Resources Technology Projects

Authority – §TGC 2054.161

6.1 On initiation of an information resources technology project, including an application development project and any information resources projects described in subchapter G of Texas Government Code §2054, each component institution shall classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements under Texas Government Code §441.185 for each classification.

7. Content of Rules of Behavior

Authority – TSUS Board of Regents

7.1 Each component institution's rules of behavior must address, at minimum, the rules established in this section.

7.2 Institutional vs. Individual Purpose

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

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

7.2.3 Rules for incidental use of institutional information resources.

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

7.3 Personal vs. Official Representation

7.3.1 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.

7.3.2 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.

7.3.3 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.

7.4 Limitations on the Availability of Information Resources

7.4.1 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 other information resources.

7.5 Privacy and Confidentiality of Electronic Documents

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

7.5.2 Information resources provided by the TSUS and its component institutions are essentially owned, respective of established copyright and intellectual law and TSUS and institutional policy, 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.

7.5.3 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:

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

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

7.5.3.3 Protect the integrity of the institution's information resources, and the rights and other property of the institution;

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

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

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

7.6 Failure to Comply with Information Technology Policies

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

7.6.1.1 Suspension or loss of access to institutional information resources;

7.6.1.2 Removal of elevated privileges to institutional information resources;

7.6.1.3 Appropriate disciplinary action under existing procedures applicable to institutional users; and

7.6.1.4 Civil or criminal prosecution.

7.6.2 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.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. Procedures

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 controls;

3.1.2 Review and update Personnel Security procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Contingency Planning procedures related to the controls in this policy.

4. Position Risk Designation

Authority - DIR CC: PS-2

4.1 Component institutions 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 Component institutions 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 and where rescreening is indicated, the frequency of rescreening.

6. Personnel Termination

Authority - DIR CC: PS-4

6.1 Component institutions, upon termination of an individual's employment or employment-like affiliation (e.g., volunteers, contractors, guest lecturers, temporary workers, interns), must:

6.1.1 Disable information system access and terminate/revoke any authenticators and 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 the terminated individual; and

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

6.2 Component institutions must establish procedures to sufficiently accommodate reasonably expected scenarios in which the controls in section 6.1 above cannot be fully executed upon the termination of an individual's employment (e.g., the termination of an employee who is also an actively enrolled student). At minimum, procedures must ensure that access and privileges associated with the terminated individual's employment or employment-like affiliation are removed even if the individual must retain access to information resources for other purposes.

7. Personnel Transfer

Authority - DIR CC: PS-5

7.1 Component institutions must:

7.1.1 Review and confirm ongoing operational need for current logical and physical access authorizations to information systems and 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 because of reassignment or transfer; and

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

8. Access Agreements

Authority - DIR CC: PS-6

8.1 Component institutions 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 Verify 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. External Personnel Security

Authority - DIR CC: PS-7

9.1 Component institutions must:

9.1.1 Establish personnel security requirements including security roles and responsibilities for external providers;

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

9.1.3 Document personnel security requirements;

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

9.1.5 Monitor provider compliance with personnel security requirements.

10. Personnel Sanctions

Authority - DIR CC: PS-8

10.1 Component institutions 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 or roles 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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

    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 controls;

    3.1.2 Review and update Risk Assessment procedures at an institution-defined frequency; and

    3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Risk Assessment procedures related to the controls in this policy.

4. **Security Categorization**

    Authority - DIR CC: RA-2, TAC 202.75, TAC 202.1

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

4.2 Component institutions must:

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

4.2.2 Identify and define institution-appropriate information classification categories including, at minimum, the definition of "Confidential Information" as specified by 1 Texas Administrative Code Chapter 202, Subchapter A;

4.2.3 Document the security categorization results, including supporting rationale, in the system security plan for each information system; and

4.2.4 Verify that security categorization decisions are reviewed and approved by the authorizing official or the authorizing official's designated representative.

5. Risk Assessment & Supply Chain Risk Assessment

Authority - DIR CC: RA-3, RA-3(1); TAC 202.75, TAC 202.77; TGC 2054.0593

5.1 Component institutions must:

5.1.1 Conduct an assessment of risk, including:

5.1.1.1 The likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of each information system and the information processed, stored, and/or transmitted, and any related information;

5.1.1.2 The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; and

5.1.1.3 The identification of threats to and vulnerabilities in each information system;

5.1.2 Integrate risk assessment results and risk management decisions from the institution and mission or business process perspectives with information system-level risk assessments;

5.1.3 Review and document risk assessment results in a report on a recurring, institution-defined frequency;

5.1.4 Disseminate risk assessment results to institution-defined personnel or roles;

5.1.5 Update the risk assessment at an institution-defined frequency or when there are significant changes to information systems, environments of operation, or other conditions that may impact the security state of information systems; and

5.1.6 Ensure risk assessments are performed by information owners and supported by information custodians:

5.1.6.1 At least biennially for systems containing confidential data;

5.1.6.2 Periodically, at a frequency determined by the institution, for systems containing non-confidential data; and

5.1.6.3 When significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system occur.

5.2 Component institutions must:

5.2.1 Assess supply chain risks associated with institution-defined systems, system components, and system services; and

5.2.2 Update the supply chain risk assessment at an institution-defined frequency when there are significant changes to the relevant supply chain, or when changes to the system, environment of operation, or other conditions may necessitate a change in the supply chain.

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

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

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

6. Vulnerability Monitoring and Scanning

Authority - DIR CC: RA-5

6.1 Component Institutions must:

6.1.1 Monitor and 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 monitoring and scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using institution-defined standards 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 from vulnerability monitoring activities and results from security assessments;

6.1.4 Remediate legitimate vulnerabilities in an institution-defined response time in accordance with an institutional assessment of risk;

6.1.5 Share information obtained from the vulnerability scanning and monitoring processes and security assessments with appropriate information system custodians in accordance with each component institution's internal dissemination procedures; and

6.1.6 Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

7. Risk Response

Authority - DIR CC: RA-7

7.1 Component Institutions must respond to findings from security assessments, monitoring, and audits in accordance with institutional risk tolerance.

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 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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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 controls;

3.1.2 Review and update System and Communications Protection procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional System and Communications Protection procedures related to the controls in this policy.

4. **Denial of Service Protection**

Authority - DIR CC: SC-5

4.1 Component institutions must protect information systems against, or limit the effects of,

institution-defined types of denial-of-service attacks by employing institution-defined safeguards.

5. **Boundary Protection**
Authority - DIR CC: SC-7

5.1 Component institutions must:

5.1.1 Monitor and control communications at the external interfaces of each information system and at key internal interfaces within each information system;

5.1.2 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal institutional 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 institutional security architecture.

5.2 Each component institution head (or their designated representative) and the institution's information security officer must establish a security strategy that includes perimeter protection. Perimeter security controls incorporated in the perimeter protection strategy may include and/or affect some or all of the following components:

5.2.1 Demilitarized Zone(s) (DMZ);

5.2.2 Firewall(s);

5.2.3 Intrusion detection system(s);

5.2.4 Intrusion prevention system(s); and

5.2.5 Router(s).

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

6.1 Component institutions must ensure that each information system protects the confidentiality and/or integrity of transmitted information.

6.2 Component institutions must:

6.2.1 Document in a Standard, based on institutional risk-management decisions, encryption requirements for data transmissions of confidential and non-confidential information and encryption key standards and management; and

6.2.2 Encrypt confidential information with, at minimum, a 128-bit encryption algorithm when the confidential information is transmitted over a public network (e.g., the Internet).

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 institution-defined requirements for key generation, distribution, storage, access, and destruction.

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

8.1 Component institutions must:

8.1.1 Determine institution-defined cryptographic uses; and

8.1.2 Implement institution-defined types of cryptography required for each specified cryptographic use.

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

9.1 Component institutions must:

9.1.1 Prohibit remote activation of collaborative computing devices and applications except for institution-defined devices and applications; 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 Component institutions must ensure that each information system that provides name resolution services:

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

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

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

11.1 Component institutions must ensure that each information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the information system receives from authoritative sources.

12. **Architecture and Provisioning for Name / Address Resolution Service**
Authority - DIR CC: SC-22

12.1 Component institutions must ensure that information systems that collectively provide name/address resolution service for a component institution are fault-tolerant and implement internal and external role separation.

13. **Protection of Information at Rest**
Authority - TSUS ISO Council: SC-28

13.1 Component institutions must protect the confidentiality and/or integrity of institution-defined types of information at rest.

13.2 Component institutions must:

13.2.1 Document in a Standard, based on institutional risk-management decisions, encryption requirements for information storage devices, as well as specific requirements for portable devices, removable media, and encryption key standards and management;

13.2.2 Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., a webserver or fileserver accessible without authentication or other access controls) must be encrypted;

13.2.3 Discourage the use of portable devices to store confidential information; and

13.2.4 Require that confidential information be encrypted if copied to or stored on:

13.2.4.1 Endpoint computing devices not owned by a state agency;

13.2.4.2 Portable computing devices (regardless of ownership); or

13.2.4.3 Removable media (regardless of ownership).

14. **Process Isolation**

Authority - DIR CC: SC-39

14.1 Component institutions must ensure that each information system maintains a separate execution domain for each executing process.

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.

Management: This policy is managed by the TSUS Information Security Council and 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.

Exceptions: Pursuant to TAC 202.71 (c), the component institution's Information Security Officer, with the approval of their agency head, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

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. **Procedures**

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

3.1 Component institutions must:

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

3.1.2 Review and update System and Information Integrity procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional System and Information Integrity procedures related to the controls in this policy

4. **Flaw Remediation**

Authority - DIR CC: SI-2

4.1 Component institutions must:

4.1.1 Identify, report to institutional personnel or roles with information security responsibilities, and correct information system flaws;

4.1.2 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 Implement, signature-based and/or non-signature based malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

5.1.2 Automatically update malicious code protection mechanisms as 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 information systems 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 an alert to institution-defined personnel or roles; and/or perform another institution-defined action.

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

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 information systems through institution-defined techniques and methods;

6.1.3 Deploy monitoring devices and/or invoke internal monitoring capabilities:

6.1.3.1 Strategically within information systems to collect institution-defined essential information; and

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

6.1.4 Analyze detected events and anomalies;

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

6.1.6 Adjust the level of information system monitoring activity whenever there is a change in risk to institutional operations and assets, individuals, or other organizations;

6.1.7 Obtain legal opinion regarding information system monitoring activities; and

6.1.8 Provide institution-defined information system monitoring information to institution-defined personnel or roles 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 Disseminate security alerts, advisories, and directives to institution-defined personnel or roles, institution-defined elements within the institution, and/or institution-defined external organizations; and

7.1.4 To the extent required by law or other regulations, implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

8. Information Input Validation

Authority - DIR CC: SI-10

8.1 Component institutions must ensure that each information system checks the validity of institution-defined information inputs.

9. Information Management and Retention

Authority - DIR CC: SI-12

9.1 Component institutions must manage and retain information within each information system and information output from each information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and operational requirements.

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.

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 throughout the system development life cycle.

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 Standards and Technology Special Publication 800-53 Version 4 (NIST SP 800-53 Rev. 4).

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.