POLICY LIT.3.05
INFORMATION SECURITY CONTROL STANDARDS

SCOPE: Faculty, Staff, Students, and Guests

1. POLICY STATEMENT

1.1. Purpose: The purpose of this policy is to define information security control standards for Lamar Institute of Technology (LIT) information systems and data, guided by required elements of the Texas Department of Information Resources Security Control Standards Catalog.

1.2. Scope: This policy applies to the Lamar Institute of Technology (LIT). All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the college's information resources.

1.3. Application: The statements in this document establish the requirements for Lamar Institute of Technology. At the discretion of the college, more stringent, restrictive, or enhanced requirements may be established.

1.4. Management: This policy is managed by the Lamar Institute of Technology Chief Information Security Officer and will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate college personnel.

2. DEFINITIONS

2.1. A listing of initialisms used in this and other information resources policies can be found in Appendix A.

2.2. A glossary with definitions of terms used in this and other information resources policies can be found in Appendix B.

3. ACCESS CONTROL

3.1. Procedures (Authority - DIR Controls Catalog (CC): AC-1)

3.1.1. LIT must:

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

3.1.1.2. Review and update Access Control procedures at a college defined frequency; and

3.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Access Control procedures related to the controls in this policy.

3.1.2. Account Management & Disable Accounts (Authority - DIR CC: AC-2, AC-2(3), TAC 202.72)

3.1.2.1. LIT must:

3.1.2.1.1. Define and document, in consultation with the college's ISO and IRM, the types of information system accounts that support organizational missions and business functions.

3.1.2.1.2. Assign account manager responsibilities for information system accounts to the respective information owner.

3.1.2.1.3. Establish conditions for group and role membership.

3.1.2.1.4. 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.

3.1.2.1.5. Require approval from the information owner for requests to create information system accounts.

3.1.2.1.6. Require the respective information custodian to create, enable, modify, disable, and remove information system accounts in accordance with college-defined procedures and conditions.

3.1.2.1.7. Require the respective information custodian to monitor the use of information system accounts.

3.1.2.1.8. Notify account managers (i.e., information owners) within a college-defined period of time for each of the following conditions:

3.1.2.1.8.1. when the accounts are no longer required;

3.1.2.1.8.2. when users are terminated or transferred; and

3.1.2.1.8.3. when individual information system usage or need-to-know changes.

3.1.2.1.9. Require that determinations to authorize access to each information system by the respective information owner are based on:

3.1.2.1.9.1. a valid access authorization request;

3.1.2.1.9.2. intended system usage; and

3.1.2.1.9.3. other attributes as required by mission or business functions.

3.1.2.1.10. 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 LIT.

3.1.2.1.11. 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.

3.1.2.1.12. Align account management processes with personnel termination and transfer processes.

3.1.2.1.13. Disable accounts within a college-defined period of time when the accounts:

3.1.2.1.13.1. Have expired,

3.1.2.1.13.2. Are no longer associated with a user or individual,

3.1.2.1.13.3. Are in violation of college policy, or

3.1.2.1.13.4. Have been inactive for a college-defined period of time.

3.1.3. Access Enforcement (Authority - DIR CC: AC-3)

3.1.3.1. LIT must ensure that information systems enforce approved authorizations for logical access to information and system resources in accordance with applicable, college-defined access control policies.

3.1.4. Separation of Duties (Authority - DIR CC: AC-5)

3.1.4.1. LIT must:

3.1.4.1.1. Identify and document separation of duties of individuals based on college-defined criteria; and

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

3.1.5. Least Privilege (Authority - DIR CC: AC-6)

3.1.5.1. LIT must:

3.1.5.1.1. Establish the principle of least privilege as a critical and strategic component of college-level information security policies and procedures; and

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

3.1.6. Unsuccessful Logon Attempts (Authority - DIR CC: AC-7).

3.1.6.1. LIT must ensure that each information system:

3.1.6.1.1. Enforces a college-defined limit of consecutive, invalid logon attempts by a user or source of authentication during a college-defined period of time; and

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

3.1.6.1.2.1. Locks the account or node for a college-defined period of time;

3.1.6.1.2.2. Locks the account or node until released by an administrator;

3.1.6.1.2.3. Delays the next logon prompt according to a college-defined delay algorithm; and/or

3.1.6.1.2.4. Notifies the information custodian.

3.1.7. System Use Notification (Authority - DIR CC: AC-8)

3.1.7.1. LIT must ensure that each information system:

3.1.7.1.1. Displays to human users at logon interfaces a college-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:

3.1.7.1.1.1. Users are accessing a college information system;

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

3.1.7.1.1.3. Unauthorized use of the information system is prohibited and subject to criminal prosecution and civil penalties; and

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

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

3.1.7.1.3. For publicly accessible systems that do not have logon interfaces:

3.1.7.1.3.1. Displays system use information under college-defined conditions before granting further access.

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

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

3.1.8. Permitted Actions Without Identification or Authentication (Authority - DIR CC: AC-14)

3.1.8.1. LIT must:

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

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

3.1.9. Remote Access (Authority - DIR CC: AC-17)

3.1.9.1. LIT must:

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

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

3.1.10. Wireless Access (Authority - DIR CC: AC-18)

3.1.10.1. LIT must:

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

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

3.1.11. Access Control for Mobile Devices (Authority - DIR CC: AC-19)

3.1.11.1. LIT must:

3.1.11.1.1. Establish configuration requirements, connection requirements, and implementation guidance for college-controlled mobile devices, to include when such devices are outside of college-controlled networks; and

3.1.11.1.2. Authorize the connection of mobile devices to college information systems.

3.1.12. Use of External Systems (Authority - DIR CC: AC-20)

3.1.12.1. LIT 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:

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

3.1.12.1.2. Process, store, or transmit college-controlled information using external information systems.

3.1.13. Publicly Accessible Content (Authority- DIR CC: AC-22)

3.1.13.1. LIT must:

3.1.13.1.1. Designate individuals authorized to make information publicly accessible;

3.1.13.1.2. Train authorized individuals to ensure that publicly accessible information does not contain non-public information;

3.1.13.1.3. Review the proposed content of information prior to posting onto publicly accessible information systems to ensure that non-public information is not included; and

3.1.13.1.4. Review the content on the publicly accessible information system for non-public information at college defined frequencies and remove such information, if discovered.

4. AWARENESS AND TRAINING

4.1. Procedures (Authority - DIR CC: AT-1, TGC 2054.519, TGC 5054.5191, TGC 2054.5192)

4.1.1. LIT must:

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

4.1.1.2. Review and update Awareness and Training procedures at a college-defined frequency; and

4.1.1.3. Designate a college employee as responsible for managing, developing, documenting, and disseminating college Awareness and Training procedures related to the controls in this policy; and

4.1.1.4. Provide information security training for all users of college 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.

4.2. Literacy Training and Awareness & Insider Threat (Authority - DIR CC: AT-2, AT-2(2), TGC 2054.519, TGC 2054.5191, TGC 2054.5192)

4.2.1. LIT must:

4.2.1.1. Provide security literacy training to:

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

4.2.1.3. New employees during the onboarding process; and

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

4.2.1.5. Update security awareness and literacy training at an institution-defined frequency; and

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

4.3. Role-Based Training (Authority - DIR CC: AT-3, TGC 2054.519, TGC 2054.5191, TGC 2054.5192)

4.3.1. LIT must:

4.3.1.1. Provide role-based security training:

4.3.1.1.1. To information resource employees with administrative privileges and responsibilities;

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

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

4.3.1.2. Update role-based training content at a college-defined frequency.

4.4. Training Records (Authority - DIR CC: AT-4, TGC 2054.519, TGC 2054.5191, TGC 2054.5192)

4.4.1. LIT must:

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

4.4.1.2. Retain individual training records for a college-defined time period.

5. AUDIT AND ACCOUNTABILITY

5.1. Procedures (Authority - DIR CC: AU-1)

5.1.1. LIT must:

5.1.1.1. Develop procedures to facilitate the implementation of the Audit and Accountability policy and associated controls;

5.1.1.2. Review and update Audit and Accountability procedures at a college-defined frequency; and

5.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Audit and Accountability procedures related to the controls in this policy.

5.2. Event Logging (Authority - DIR CC: AU-2)

5.2.1. LIT must:

5.2.1.1. 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;

5.2.1.2. 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 college's Standard;

5.2.1.3. Require information owners and information custodians to coordinate with the college's ISO (or their designee) to coordinate event logging functions;

5.2.1.4. 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;

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

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

5.2.2. LIT must:

5.2.2.1. 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;

5.2.2.2. 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

5.2.2.3. 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

5.3. Content of Audit Records (Authority - DIR CC: AU-3)

5.3.1. LIT must ensure that each information system's audit records contain the following information:

5.3.1.1. What type of event occurred;

5.3.1.2. When the event occurred;

5.3.1.3. Where the event occurred;

5.3.1.4. Source of the event;

5.3.1.5. Outcome of the event; and

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

5.3.2. Events should contain all information needed to determine the logical location of the user.

5.4. Audit Log Storage Capacity (Authority - DIR CC: AU-4)

5.4.1. LIT must allocate audit-log storage capacity to accommodate the college's audit log retention requirements.

5.5. Response to Audit Logging Process Failures (Authority - DIR CC: AU-5)

5.5.1. LIT must:

5.5.1.1. 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;

5.5.1.2. 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

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

5.6. Audit Review, Analysis, and Reporting (Authority - DIR CC: AU-6)

5.6.1. LIT must:

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

5.6.1.2. 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

5.6.1.3. 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.

5.7. Time Stamps (Authority - DIR CC: AU-8)

5.7.1. LIT must:

5.7.1.1. Configure each information system to:

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

5.7.1.1.2. Synchronize internal system clocks with an authoritative source of time specified by the ISO and IRM;

5.7.1.2. Ensure that audit records record time stamps in milliseconds and:

5.7.1.2.1. Use Coordinated Universal Time;

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

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

5.8. Protection of Audit Information (Authority - DIR CC: AU-9)

5.8.1. LIT must protect audit information and audit tools from unauthorized access, modification, and deletion.

5.9. Audit Record Retention (Authority - DIR CC: AU-11)

5.9.1. LIT must:

5.9.1.1. Ensure records retention policies for audit records meets regulatory and college information retention requirements; and

5.9.1.2. 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.

5.10. Audit Record Generation (Authority - DIR CC: AU-12)

5.10.1. LIT must ensure that information systems:

5.10.1.1. Provide audit record generation capability for the auditable events required by this policy and related college policies and standards;

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

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

6. ASSESSMENT, AUTHORIZATION AND MONITORING POLICY

6.1. Procedures (Authority - DIR CC: CA-1)

6.1.1. LIT must:

6.1.1.1. Develop procedures to facilitate the implementation of the Security Assessment, Authorization, and Monitoring policy and associated controls;

6.1.1.2. Review and update Security Assessment, Authorization, and Monitoring procedures at a college-defined frequency; and

6.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Assessment, Authorization, and Monitoring procedures related to the controls in this policy.

6.2. Control Assessments (Authority - DIR CC: CA-2)

6.2.1. LIT must:

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

6.2.1.1.1. Controls and control enhancements under assessment;

6.2.1.1.2. Assessment procedures to be used to determine control effectiveness; and

6.2.1.1.3. Assessment environment, assessment team, and assessment roles and responsibilities;

6.2.1.2. 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;

6.2.1.3. Assess the controls in the information system and its environment of operation on a recurring frequency established by the college’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;

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

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

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

6.3. Information Exchange (Authority - DIR CC: CA-3)

6.3.1. LIT must:

6.3.1.1. Through relevant information system owners, authorize the exchange of information (i.e., interconnections) between college information systems and other information systems, including those external to the college;

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

6.3.1.2.1. Interface characteristics;

6.3.1.2.2. Security requirements, controls, and responsibilities;

6.3.1.2.3. Information system category; and

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

6.3.2. Regularly review and update as necessary established Interconnection Security Agreements at the time of periodic risk assessments or at a college-defined frequency.

6.4. Plan of Action and Milestones (Authority - DIR CC: CA-5)

6.4.1. LIT must:

6.4.1.1. Develop a Plan of Action and Milestones for each information system to document the college'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

6.4.1.2. Update existing plans of action and milestones at a college-defined frequency based on the findings from controls assessments, audits, and continuous monitoring activities.

6.5. Authorization (Authority - DIR CC: CA-6)

6.5.1. LIT must:

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

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

6.5.1.3. 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;

6.5.1.4. Ensure that the Authorizing Official for common controls authorizes the use of those controls for inheritance by college information systems; and

6.5.1.5. Update the security authorization at the time of periodic risk assessment for the information system or at a college-defined frequency.

6.6. Continuous Monitoring & Risk Monitoring (Authority - DIR CC: CA-7, CA-7(4))

6.6.1. LIT must develop a continuous monitoring strategy and implement an information system-level continuous monitoring program that includes:

6.6.1.1. Establishment of system-level metrics to be monitored;

6.6.1.2. Establishment of frequencies for monitoring and for control assessments supporting such monitoring;

6.6.1.3. Ongoing control assessments in accordance with the college continuous monitoring strategy;

6.6.1.4. Ongoing monitoring of information system and college-defined metrics in accordance with the college continuous monitoring strategy;

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

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

6.6.1.7. Reporting the security status of each information system to appropriate stakeholders at a college-defined frequency.

6.6.2. LIT must ensure that risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

6.6.2.1. Effectiveness monitoring;

6.6.2.2. Compliance monitoring; and

6.6.2.3. Change monitoring.

6.7. Penetration Testing (Authority - DIR CC: CA-8; TGS §2054.516(a)(2))

6.7.1. LIT must conduct penetration testing at a college-defined frequency on college-defined information systems and information system components.

6.7.2. LIT must ensure that:

6.7.2.1. 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 a college-defined frequency; and

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

6.8. Internal System Connections (Authority - DIR CC: CA-9)

6.8.1. LIT must:

6.8.1.1. Authorize internal connections of college-defined information system components or classes of components to each information system;

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

6.8.1.3. Terminate internal system connections based on college-defined conditions; and

6.8.1.4. Review the need for each internal connection at a college-defined frequency.

7. CONFIGURATION MANAGEMENT

7.1. Procedures (Authority - DIR CC: CM-1)

7.1.1. LIT must:

7.1.1.1. Develop procedures to facilitate the implementation of the Configuration Management policy and associated controls;

7.1.1.2. Review and update Configuration Management procedures at a college-defined frequency; and

7.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Configuration Management procedures related to the controls in this policy.

7.2. Baseline Configuration (Authority - DIR CC: CM-2)

7.2.1. LIT must:

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

7.2.1.2. Review and update the baseline configuration of each information system:

7.2.1.2.1. At a college-defined frequency;

7.2.1.2.2. When required because of college-defined circumstances; and

7.2.1.2.3. When information system components are installed or upgraded.

7.3. Configuration Change Control (Authority - DIR CC: CM- 3

7.3.1. LIT must:

7.3.1.1. Determine and document the types of changes to information systems that are configuration-controlled;

7.3.1.2. Review proposed configuration-controlled changes to information systems and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

7.3.1.3. Document configuration change decisions associated with the information systems;

7.3.1.4. Implement approved configuration-controlled changes to the information systems;

7.3.1.5. Retain records of configuration-controlled changes to information systems for an institution-defined period of time;

7.3.1.6. Monitor and review activities associated with configuration-controlled changes to information systems; and

7.3.1.7. Coordinate and provide oversight for configuration change control activities through college-defined configuration change control elements that convenes at a college-defined frequency and/or when college-denied configuration change conditions are met.

7.3.2. LIT must ensure that all security-related information resources changes are approved by the information owner (or designee) through a change control process.

7.4. Impact Analyses (Authority - DIR CC: CM- 4)

7.4.1. LIT must analyze changes to each information system to determine potential security impacts prior to change implementation.

7.4.2. LIT must ensure that:

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

7.4.2.2. Such approval occurs prior to implementation by the college or independent contractors.

7.5. Access Restrictions for Change (Authority - DIR CC: CM- 5)

7.5.1. LIT must define, document, approve, and enforce physical and logical access restrictions associated with changes to each information system.

7.6. Configuration Settings (Authority - DIR CC: CM- 6)

7.6.1. LIT must:

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

7.6.1.2. Implement the configuration settings;

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

7.6.1.4. Monitor and control changes to the configuration settings in accordance with college policies and procedures.

7.7. Least Functionality (Authority - DIR CC: CM- 7)

7.7.1. LIT must:

7.7.1.1. Configure each information system to provide only college-defined, mission-essential capabilities; and

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

7.8. System Component Inventory (Authority - DIR CC: CM- 8)

7.8.1. LIT must:

7.8.1.1. Develop and document an inventory of information system components that:

7.8.1.1.1. Accurately reflects the information system;

7.8.1.1.2. Includes all components within each information system;

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

7.8.1.1.4. Includes college-defined information deemed necessary to achieve effective information system component accountability.

7.8.1.2. Review and update the information system component inventory at a college-defined frequency.

7.9. Software Usage Restrictions (Authority - DIR CC: CM- 10)

7.9.1. LIT must:

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

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

7.9.1.3. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

7.10. User-Installed Software (Authority - DIR CC: CM- 11)

7.10.1. LIT must:

7.10.1.1. Establish college-defined policies governing the installation of software by users;

7.10.1.2. Enforce software installation policies through college-defined methods; and

7.10.1.3. Monitor policy compliance at college-defined frequency.

8. CONTINGENCY PLANNING

8.1. Procedures (Authority -DIR CC: CP-1)

8.1.1. LIT must:

8.1.1.1. Develop procedures to facilitate the implementation of the Contingency Planning policy and associated controls;

8.1.1.2. Review and update Contingency Planning procedures at a college-defined frequency;

8.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Contingency Planning procedures related to the controls in this policy; and

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

8.2. Contingency Plan (Authority - DIR CC: CP-2)

8.2.1. LIT must:

8.2.1.1. Develop a contingency plan for each information system that:

8.2.1.1.1. Identifies essential missions and business functions and associated contingency requirements;

8.2.1.1.2. Provides recovery objectives, restoration priorities, and metrics;

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

8.2.1.1.4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

8.2.1.1.5. Addresses eventual, full information system restoration without deterioration of the controls originally planned and implemented; and

8.2.1.1.6. Is reviewed and approved by college designated personnel or roles;

8.2.1.2. Distribute copies of the contingency plan to college designated key contingency personnel (identified by name and/or by role) and college elements;

8.2.1.3. Coordinate contingency planning activities with incident handling activities;

8.2.1.4. Review the contingency plan for each information system at a college-defined frequency;

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

8.2.1.6. Communicate contingency plan changes to college designated key contingency personnel (identified by name and/or by role) and college elements; and

8.2.1.7. Protect the contingency plan from unauthorized disclosure and modification.

8.3. Contingency Training (Authority - DIR CC: CP-3)

8.3.1. LIT must provide contingency training to information system users consistent with assigned roles and responsibilities:

8.3.1.1. Within a college-defined time period of assuming a contingency role or responsibility;

8.3.1.2. When required by information system changes; and

8.3.1.3. On a college-defined frequency thereafter.

8.4. Contingency Plan Testing (Authority - DIR CC: CP-4)

8.4.1. LIT must:

8.4.1.1. Test the contingency plan for information systems at least annually using college-defined tests to determine the effectiveness of the plan and the college readiness to execute the plan;

8.4.1.2. Review the contingency plan test results; and

8.4.1.3. Initiate corrective actions, if needed.

8.5. Alternate Storage Site (Authority - DIR CC: CP-6)

8.5.1. LIT must:

8.5.1.1. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information; and

8.5.1.2. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

8.6. Telecommunications Services (Authority - DIR CC: CP-8)

8.6.1. LIT must establish alternate telecommunications services, including necessary agreements to permit the resumption of college-defined information system operations for essential mission and business functions within an college-defined period of time when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

8.7. System Backup (Authority - DIR CC: CP-9)

8.7.1. LIT must:

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

8.7.1.2. User-level information contained in information systems;

8.7.1.3. System-level information contained in information systems; and

8.7.1.4. Information system documentation, including security-related documentation;

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

8.8. System Recovery and Reconstitution (Authority - DIR CC: CP-10)

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

8.9. Alternate Communications Protocols (Authority - DIR CC: CP-11)

8.9.1. LIT must have the capability to employ college-defined alternative communications protocols in support of maintaining continuity of operations.

9. IDENTIFICATION AND AUTHENTICATION

9.1. Procedures (Authority - DIR CC: IA-1)

9.1.1. LIT must:

9.1.1.1. Develop procedures to facilitate the implementation of the Identification and Authentication policy and associated controls;

9.1.1.2. Review and update Identification and Authentication procedures at a college-defined frequency; and

9.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Identification and Authentication procedures related to the controls in this policy.

9.2. 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)

9.2.1. LIT must ensure that information systems uniquely identify and authenticate college users or processes acting on behalf of college users prior to granting the user or process access to a given information system.

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

9.2.2. LIT must implement multifactor authentication for access to privileged accounts on college information systems.

9.2.3. LIT must implement multifactor authentication for access to non-privileged accounts on college information systems.

9.3. Identifier Management (Authority - DIR CC: IA-4)

9.3.1. LIT must manage information system identifiers by:

9.3.1.1. Receiving authorization from college-defined personnel to assign an individual, group, role, service, or device identifier;

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

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

9.3.1.4. Preventing reuse of identifiers for a college-defined time period.

9.3.2. LIT must ensure a user's access authorization is appropriately modified or removed when the user's employment, job responsibilities, or affiliation with the college changes.

9.4. Authenticator Management (Authority - DIR CC: IA-5)

9.4.1. LIT must manage information system authenticators by:

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

9.4.1.2. Establishing initial authenticator content for authenticators defined by the college;

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

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

9.4.1.5. Changing default authenticators prior to first use;

9.4.1.6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

9.4.1.7. Changing or refreshing authenticators at a college-defined time period by authenticator type;

9.4.1.8. Protecting authenticator content from unauthorized disclosure and modification;

9.4.1.9. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and

9.4.1.10. Changing authenticators for group or role accounts when membership to those accounts changes.

9.5. Password-based Authentication (Authority - DIR CC: IA-5(1))

9.5.1. For password-based authentication, LIT must:

9.5.1.1. Maintain a list of commonly used, expected, or compromised passwords and update the list at a college-defined frequency and when college passwords are suspected to have been compromised directly or indirectly;

9.5.1.2. Verify, when users create or update passwords, that the passwords are not found on the college-defined list of commonly used, expected, or compromised passwords;

9.5.1.3. Transmit passwords only over cryptographically protected channels;

9.5.1.4. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

9.5.1.5. Require immediate selection of a new password upon account recovery;

9.5.1.6. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

9.5.1.7. Employ automated tools to assist the user in selecting strong password authenticators; and

9.5.1.8. Enforce college-defined password composition and complexity rules.

9.6. Authenticator Feedback (Authority - DIR CC: IA-6)

9.6.1. LIT must ensure that information systems obscure feedback of authentication information entered during authentication processes.

9.7. Cryptographic Module Authentication (Authority - DIR CC: IA-7)

9.7.1. LIT must:

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

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

9.8. Identification and Authentication (Non-Organizational Users) (Authority - DIR CC: IA-8)

9.8.1. LIT must ensure that information systems uniquely identify and authenticate non-college users or processes acting on behalf of non-college users.

9.9. Re-Authentication (Authority - DIR CC: IA-11)

9.9.1. LIT must document a Standard defining the circumstances or situations which require users to re-authenticate.

9.9.2. LIT must require users to re-authenticate according to the component college's Standard.

9.9.3. LIT's standard for re-authentication must include the following minimum requirements:

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

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

10. INCIDENT RESPONSE

10.1. Procedures (Authority - DIR CC: IR-1)

10.1.1. LIT must:

10.1.1.1. Develop procedures to facilitate the implementation of the Incident Response policy and associated controls; and

10.1.1.2. Review and update Incident Response procedures at a college-defined frequency; and

10.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Incident Response procedures related to the controls in this policy.

10.1.1.4. LIT 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.

10.2. Incident Response Training (Authority - DIR CC: IR-2)

10.2.1. LIT must provide incident response training to information system users consistent with their assigned roles and responsibilities:

10.2.1.1. Within a college-defined time period of assuming an incident response role or responsibility or acquiring information system access;

10.2.1.2. When required by information system changes; and

10.2.1.3. At an annual frequency thereafter.

10.3. Incident Response Testing (Authority - DIR CC: IR-3)

10.3.1. LIT must test the effectiveness of the incident response capability for each information system at a college-defined frequency using the college-defined tests for each information system.

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

10.4.1. LIT must:

10.4.1.1. 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

10.4.1.2. Coordinate incident handling activities with contingency planning activities;

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

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

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

10.5.1. LIT must track and document security and supply chain incidents.

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

10.6.1. LIT must:

10.6.1.1. Require personnel to report suspected security and supply chain incidents to the college's ISO (or their designee) using college-defined procedures within a college-defined time period;

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

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

10.6.1.3.1. Propagate to other state information systems;

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

10.6.1.3.3. Involve the unauthorized disclosure or modification of confidential information; or

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

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

10.6.2. 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 college’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.

10.7. Incident Response Assistance (Authority - DIR CC: IR-7)

10.7.1. LIT must provide an incident response resource, integral to the college’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 the college’s ISO and may be comprised of technical support personnel, verified third-party consultants, and other resources.

10.8. Incident Response Plan (Authority - DIR CC: IR-8)

10.8.1. LIT must:

10.8.1.1. Develop an incident response plan that:

10.8.1.2. Provides the college with a roadmap for implementing its incident response capability;

10.8.1.3. Describes the structure and organization of the incident response capability;

10.8.1.4. Provides a high-level approach for how the incident response capability fits in to the overall college;

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

10.8.1.6. Defines reportable incidents;

10.8.1.7. Provides metrics for measuring the incident response capability within the college;

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

10.8.1.9. Is reviewed and approved by appropriate, college-defined leadership; and

10.8.1.10. Explicitly designates responsibility for incident response to college-defined roles.

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

10.8.1.12. Update the incident response plan to address system and college changes or problems encountered during plan implementation, execution, or testing;

10.8.1.13. Communicate changes to the incident response plan to college elements charged with incident response responsibilities defined by name and/or role; and

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

10.9. Information Spillage Response (Authority - DIR CC: IR-9)

10.9.1. LIT must respond to information spills by:

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

10.9.1.2. Identifying the specific information involved in the information system contamination;

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

10.9.1.4. Isolating the contaminated information system or information system component;

10.9.1.5. Eradicating the information from the contaminated information system or component;

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

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

11. MAINTENANCE

11.1. Procedures (Authority - DIR CC: MA-1)

11.1.1. LIT must:

11.1.1.1. Develop procedures to facilitate the implementation of the Maintenance policy and associated controls;

11.1.1.2. Review and update Maintenance procedures at a college-defined frequency; and

11.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Maintenance procedures related to the controls in this policy.

11.2. Controlled Maintenance (Authority - DIR CC: MA-2)

11.2.1. LIT must require information custodians to:

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

11.2.1.2. 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;

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

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

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

11.2.1.6. Update appropriate college maintenance records following maintenance, repair, and/or replacement actions.

11.3. Nonlocal Maintenance (Authority - DIR CC: MA-4)

11.3.1. LIT, directly or contractually, must:

11.3.1.1. Approve and monitor nonlocal maintenance and diagnostic activities;

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

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

11.3.1.4. Maintain records for nonlocal maintenance and diagnostic activities; and

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

11.4. Maintenance Personnel (Authority - DIR CC: MA-5)

11.4.1. LIT must:

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

11.4.1.2. Verify that non-escorted personnel performing maintenance on information systems possess the required access authorizations; and

11.4.1.3. Designate college personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

12. MEDIA PROTECTION

12.1. Procedures (Authority - DIR CC: MP-1)

12.1.1. LIT must:

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

12.1.1.2. Review and update Media Protection procedures at a college-defined frequency; and

12.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Media Protection procedures related to the controls in this policy.

12.2. Media Access (Authority - DIR CC: MP-2)

12.2.1. LIT must restrict access to college-defined types of digital and non-digital media to college-defined personnel or roles.

12.3. Media Sanitization & Review, Approve, Track, Document, and Verify (Authority - Texas Government Code (TGC) 441.185; DIR CC: MP-6, MP-6(1))

12.3.1. LIT must:

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

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

12.3.2. LIT must review, approve, track, document, and verify media sanitization and disposal actions.

12.3.3. LIT must keep a record documenting the removal and completion of sanitization of media that stored confidential information with the following information:

12.3.3.1. Date;

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

12.3.3.3. Inventory number(s);

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

12.3.3.5. The name and address of the organization to which the media were transferred.

12.4. Media Use (Authority - DIR CC: MP-7)

12.4.1. LIT must document and enforce a Standard defining at minimum:

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

12.4.1.2. 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

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

12.4.2. Each component college must prohibit the use of portable storage devices in college systems when such devices have no identifiable owner.

13. PHYSICAL AND ENVIRONMENTAL PROTECTION

13.1. Procedures (Authority - DIR CC: PE-1)

13.1.1. LIT must:

13.1.1.1. Develop procedures to facilitate the implementation of the Physical and Environmental Protection policy and associated controls;

13.1.1.2. Review and update Physical and Environmental Protection procedures at a college-defined frequency; and

13.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Physical and Environmental Protection procedures related to the controls in this policy.

13.2. Physical Access Authorizations (Authority - DIR CC: PE-2)

13.2.1. LIT must:

13.2.1.1. Develop, approve, and maintain a list of individuals with authorized access to facilities in which one or more college information systems reside;

13.2.1.2. Issue authorization credentials for facility access;

13.2.1.3. Review the access list detailing authorized facility access by individuals at a college-defined frequency; and

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

13.3. Physical Access Control (Authority - DIR CC: PE-3)

13.3.1. LIT must:

13.3.1.1. Enforce physical access authorizations at college-defined entry and exit points to facilities in which one or more college information systems reside by:

13.3.1.1.1. Verifying individual access authorizations before granting access to each facility; and

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

13.3.1.2. Maintain physical access audit logs for college-defined entry and exit points;

13.3.1.3. Control access to areas within each facility designated as publicly accessible using college-defined controls;

13.3.1.4. Escort visitors and monitor visitor activity based on college-defined requirements;

13.3.1.5. Secure keys, combinations, and other physical access devices;

13.3.1.6. Inventory college-defined physical access devices at a college-defined frequency; and

13.3.1.7. Change combinations and keys:

13.3.1.7.1. At a college-defined frequency; and/or

13.3.1.7.2. When keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

13.4. Monitoring Physical Access (Authority - DIR CC: PE-6)

13.4.1. LIT must:

13.4.1.1. Monitor physical access to facilities in which one or more college information systems reside to detect and respond to physical security incidents;

13.4.1.2. Review physical access logs at a college-defined frequency and upon occurrence of college-defined events or potential indications of events; and

13.4.1.3. Coordinate results of reviews and investigations with the college incident response capability.

13.5. Visitor Access Records (Authority - DIR CC: PE-8)

13.5.1. LIT must:

13.5.1.1. Maintain visitor access records to facilities in which one or more college information systems reside for a college-defined period;

13.5.1.2. Review visitor access records at a college-defined frequency; and

13.5.1.3. Report anomalies in visitor access records to college-defined personnel.

13.6. Emergency Lighting (Authority - DIR CC: PE-12)

13.6.1. LIT 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 college information systems reside.

13.7. Fire Protection (Authority - DIR CC: PE-13)

13.7.1. LIT must employ and maintain fire suppression and detection devices or systems for facilities in which one or more college information systems reside that are supported by an independent energy source.

13.8. Environmental Controls (Authority - DIR CC: PE-14)

13.8.1. LIT must:

13.8.1.1. Maintain temperature and humidity levels within facilities in which one or more college information systems reside at college-defined acceptable levels; and

13.8.1.2. Monitor environmental control levels at a college-defined frequency.

13.9. Water Damage Protection (Authority - DIR CC: PE-15)

13.9.1. LIT must protect facilities in which one or more college 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.

13.10. Delivery and Removal (Authority - DIR CC: PE-16)

13.10.1. LIT must:

13.10.1.1. Authorize and control college-defined types of information system components entering and exiting facilities in which one or more college information systems reside; and

13.10.1.2. Maintain records of college-defined information system components.

13.11. Alternate Work Site (Authority - DIR CC: PE-17)

13.11.1. LIT must:

13.11.1.1. Determine and document college-defined alternate work sites allowed for use by employees;

13.11.1.2. Employ college-defined controls at alternate work sites;

13.11.1.3. Assess the effectiveness of controls at alternate work sites; and

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

14. SECURITY PLANNING

14.1. Procedures (Authority - DIR CC: PL-1, TAC 202.73)

14.1.1. LIT must:

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

14.1.1.2. Review and update Security Planning procedures at a college-defined frequency; and

14.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Security Planning procedures related to the controls in this policy.

14.1.2. LIT's information security officer must report annually on the LIT information security program to the President in compliance with 1 Texas Administrative Code §202.73(a).

14.2. System Security and Privacy Plans (Authority - DIR CC: PL-2)

14.2.1. LIT must ensure that each information system under the college's custodianship has a corresponding System Security Plan that:

14.2.1.1. Is consistent with the college's enterprise architecture;

14.2.1.2. Explicitly defines the constituent information system component(s);

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

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

14.2.1.5. Describes any specific threats to the information system that are of concern to the college;

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

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

14.2.1.8. Identifies any relevant security control baselines and, if applicable, college-defined overlays;

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

14.2.1.10. Includes risk determinations for security architecture and design decisions;

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

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

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

14.2.3. LIT must review and update System Security Plans on a recurring basis. This review must occur at a college-defined frequency or when changes to the information system or System Security Plan require it.

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

14.3. Rules of Behavior & Social Media and External Site/Application Usage Restrictions (Authority - DIR CC: PL-4, PL-4(1))

14.3.1. LIT must:

14.3.1.1. 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 college information resources that describes the users' responsibilities and expected behavior for the usage and security of information and Information Resources;

14.3.1.2. Periodically review and update the college acceptable use policy;

14.3.1.3. Require college 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

14.3.1.4. 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.

14.3.2. LIT must include in the rules of behavior restrictions on:

14.3.2.1. Use of social media, social networking sites, and external sites/applications;

14.3.2.2. Posting college information on public websites; and

14.3.2.3. Use of college-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

14.4. Baseline Selection (Authority - DIR CC: PL-10)

14.4.1. LIT must:

14.4.1.1. Select a control baseline for information systems; and

14.4.1.2. Use the controls contained in the DIR Security Controls Standards Catalog as the default baseline for information systems.

14.5. Baseline Tailoring (Authority - DIR CC: PL-11)

14.5.1. LIT must tailor the selected control baseline by applying college-defined tailoring actions.

14.6. Data Classification, Security, and Retention Requirements for Information Resources Technology Projects (Authority – §TGC 2054.161)

14.6.1. 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, the college 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.

14.7. Content of Rules of Behavior (Authority – TSUS Board of Regents)

14.7.1. LIT's rules of behavior must address, at minimum, the rules established in this section.

14.7.2. Institute vs. Individual Purpose

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

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

14.7.2.3. Rules for incidental use of college information resources.

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

14.7.3. Personal vs. Official Representation

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

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

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

14.7.4. Limitations on the Availability of Information Resources

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

14.7.5. Privacy and Confidentiality of Electronic Documents

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

14.7.5.2. Information resources provided by the TSUS and LIT are essentially owned, respective of established copyright and intellectual law and TSUS and college policy, by the State of Texas and subject to state oversight. Consequently, persons have no right to privacy in their use of college information resources even when using a personal or third-party device to access such resources.

14.7.5.3. LIT should take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons using college information resources that the college will not seek access to their electronic messages or documents without their prior consent except where necessary to:

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

14.7.5.3.2. Allow college officials to fulfill their responsibilities when acting in their assigned capacity;

14.7.5.3.3. Protect the integrity of the college's information resources, and the rights and other property of the college;

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

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

14.7.5.4. LIT 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 college.

14.7.5.5. Failure to Comply with Information Technology Policies

14.7.5.6. Failure to adhere to the provisions of TSUS IT policies or the IT policies of LIT may result in:

14.7.5.6.1. Suspension or loss of access to college information resources;

14.7.5.6.2. Removal of elevated privileges to college information resources;

14.7.5.6.3. Appropriate disciplinary action under existing procedures applicable to college users; and

14.7.5.6.4. Civil or criminal prosecution.

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

15. PROGRAM MANAGEMENT

15.1. Information Security Program Plan (Authority - DIR CC: PM-1)

15.1.1. LIT must:

15.1.1.1. Develop and disseminate a college-wide information security program plan that:

15.1.1.1.1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

15.1.1.1.2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among college entities, and compliance;

15.1.1.1.3. Reflects the coordination among college entities responsible for information security; and

15.1.1.1.4. Is approved by a senior official with responsibility and accountability for the risk being incurred to college operations (including missions, functions, image, and reputation), college assets, and individuals;

15.1.1.2. Review the college-wide information security program plan at a college-defined frequency;

15.1.1.3. Update the information security program plan to address institutional changes and problems identified during plan implementation or control assessments; and

15.1.1.4. Protect the information security program plan from unauthorized disclosure and modification.

15.2. Information Security Program Leadership Role (Authority - DIR CC: PM-2, Texas Administrative Code (TAC) 202.71, TAC 202.74)

15.2.1. LIT must:

15.2.1.1. Appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a college-wide information security program approved by the college's President or delegate.

15.2.1.2. LIT's senior information security officer is charged with the responsibilities enumerated at Texas Government Code §2054.136 and 1 Texas Administrative Code §202.71.

15.3. Information Security Resources (Authority - DIR CC: PM-3)

15.3.1. LIT must:

15.3.1.1. Include the resources needed to implement the information security program in capital planning and investment requests and document all exceptions to this requirement;

15.3.1.2. Prepare documentation required for addressing the information security program in capital planning and investment requests in accordance with applicable laws, regulations, policies and standards; and

15.3.1.3. Make available for expenditure, the planned information security resources.

15.4. Plan of Action and Milestones Process (Authority - DIR CC: PM-4)

15.4.1. LIT must:

15.4.1.1. Implement a process to ensure that plans of action and milestones for the information security program and associated college information systems:

15.4.1.1.1. Are developed and maintained;

15.4.1.1.2. Document the remedial information security actions to adequately respond to risk to college operations and assets, individuals, and other organizations; and

15.4.1.1.3. Are reported in accordance with college-defined reporting requirements.

15.4.1.2. Review plans of action and milestones for consistency with the college risk management strategy and college-wide priorities for risk response actions.

15.5. Information System Inventory (Authority - DIR CC: PM-5)

15.5.1. LIT must develop and update, on a college-defined frequency, an inventory of college information systems.

15.6. Information Security Measures of Performance (Authority - DIR CC: PM-6)

15.6.1. LIT must develop, monitor, and report to college-defined individuals on the results of information security measures of performance.

15.7. Enterprise Architecture (Authority - DIR CC: PM-7)

15.7.1. LIT must develop an enterprise architecture with consideration for information security and the resulting risk to college operations, college assets, individuals, and other organizations.

15.8. Risk Management Strategy (Authority - DIR CC: PM-9)

15.8.1. LIT must:

15.8.1.1. Develop a comprehensive strategy to manage:

15.8.1.1.1. Security risk to college operations and assets, individuals, and other college information systems; and

15.8.1.1.2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information.

15.8.1.2. Implement the risk management strategy consistently across the college; and

15.8.1.3. Review and update the risk management strategy on a college-defined frequency or as required to address college changes.

15.9. Authorization Process (Authority - DIR CC: PM-10)

15.9.1. LIT must:

15.9.1.1. Manage the security of college information systems and the environments in which those systems operate through authorization processes;

15.9.1.2. Designate individuals to fulfill specific roles and responsibilities within the college risk management process; and

15.9.1.3. Integrate the authorization process into a college-wide risk management program.

15.10. Testing, Training, and Monitoring (Authority - DIR CC: PM-14)

15.10.1. LIT must:

15.10.1.1. Implement a process for ensuring that college plans for conducting security testing, training, and monitoring activities associated with college information systems:

15.10.1.1.1. Are developed and maintained; and

15.10.1.1.2. Continue to be executed; and

15.10.1.2. Review testing, training, and monitoring plans for consistency with the college risk management strategy and college-wide priorities for risk response actions.

15.11. Security Groups and Associations (Authority - DIR CC: PM-15)

15.11.1. LIT must establish and institutionalize contact with selected groups and associations within the information security community:

15.11.1.1. To facilitate ongoing information security education and training for college information security personnel;

15.11.1.2. To maintain currency with recommended information security practices, techniques, and technologies; and

15.11.1.3. To share current information security information, including threats, vulnerabilities, and incidents.

15.12. Threat Awareness Program (Authority - DIR CC: PM-16)

15.12.1. LIT must implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

15.13. Information Systems Governance and Management (Authority – TSUS ISO Council; TAC 202)

15.13.1. LIT must define a management framework which clearly delineates the roles and responsibilities for the management of college information systems.

15.13.2. At minimum, each LIT information system management framework must:

15.13.2.1. Delineate distinct roles for the information owner and information custodian of each information system;

15.13.2.2. Establish the responsibilities of information owners to include:

15.13.2.2.1. Duties ascribed by TAC 202.72; and

15.13.2.2.2. Assurance of compliance with state and college standards.

15.13.2.3. Establish the responsibilities of information custodians to include:

15.13.2.3.1. Duties ascribed by TAC 202.72; and

15.13.2.3.2. Assurance of compliance with state and college standards.

15.13.3. Establish the responsibilities of all information system users to, at minimum, require users to:

15.13.3.1. Use the information system or other information resource only for the purpose specified by the college or information owner;

15.13.3.2. Comply with information security controls and college policies, including those designed to prevent unauthorized or accidental disclosure, modification, or destruction of information and information resources; and

15.13.3.3. Formally acknowledge that they will comply with the security policies and procedures in a method determined by the college President or their designated representative.

15.13.3.4. Incorporate threat and incident response procedures as specified in the TSUS Incident Response Policy.

15.13.3.5. Incorporate oversight measures including, but not limited to, obligations outlined in the TSUS "System and Services Acquisition" and "Risk Assessment" policies.

15.14. Network Governance and Management (Authority - TSUS ISO Council; TAC 202)

15.14.1. LIT must define a management framework which clearly delineates the roles and responsibilities for the management of college information networks.

15.14.2. At minimum, LIT's network management framework must:

15.14.2.1. Delineate distinct roles for the ownership and custodianship of the college's network;

15.14.2.2. Assign administration of the college network by the Information Resources Manager (IRM) or their designee;

15.14.2.3. Ensure owners, custodians, and users of the college network and the devices and information systems connected to the college network understand their accountability for such use, including, but not limited to, the Rules of Behavior as specified in the "Planning" TSUS IT Policy.

15.14.2.4. Incorporate design and architectural planning and coordination measures to, at minimum, include the following:

15.14.2.4.1. Appropriate logical and/or physical segmentation of elements of the college network to promote sufficient separation of traffic based on security principles and performance purposes as authorized by each component institution's ISO.

15.14.2.4.2. Fault tolerance in critical components of the network and upstream service providers to mitigate risks to network availability;

15.14.2.4.3. Institute-defined procedures for the management of network-based security devices;

15.14.2.4.4. Procedures for the management of public IP addresses assigned to the component institution by the American Registry for Internet Numbers (ARIN) and/or other external entities, including, at minimum, maintenance of up-to-date points of contact;

15.14.2.4.5. Institute-defined procedures to ensure 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;

15.14.2.4.6. Institute-defined procedures to ensure incident response actions comply with established, policy-defined controls and best practices regarding the preservation and treatment of forensic data;

15.14.2.4.7. Adherence to the requirements set forth in the “Configuration Management” TSUS IT Policy;

15.14.2.4.8. Implementation of safeguards as required by the “System and Communication Protection” TSUS IT Policy; and

15.14.2.4.9. Procedures to regularly conduct security and risk assessments in alignment with relevant policies and laws, including the “Risk Assessment” TSUS IT Policy.

16. PERSONNEL SECURITY POLICY

16.1. Procedures (Authority - DIR CC: PS-1)

16.1.1. LIT must:

16.1.1.1. Develop procedures to facilitate the implementation of the Personnel Security policy and associated controls;

16.1.1.2. Review and update Personnel Security procedures at a college-defined frequency; and

16.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Contingency Planning procedures related to the controls in this policy.

16.2. Position Risk Designation (Authority - DIR CC: PS-2)

16.2.1. LIT must:

16.2.1.1. Assign a risk designation to all college positions;

16.2.1.2. Establish screening criteria for individuals filling those positions; and

16.2.1.3. Review and update position risk designations at a college-defined frequency.

16.3. Personnel Screening (Authority - DIR CC: PS-3)

16.3.1. LIT must:

16.3.1.1. Screen individuals prior to authorizing access to information systems; and

16.3.1.2. Rescreen individuals when college-defined conditions require rescreening and where rescreening is indicated, the frequency of rescreening.

16.4. Personnel Termination (Authority - DIR CC: PS-4)

16.4.1. LIT, upon termination of an individual’s employment or employment-like affiliation (e.g., volunteers, contractors, guest lecturers, temporary workers, interns), must:

16.4.1.1. Disable information system access and terminate/revoke any authenticators and credentials associated with the individual within a college-defined time period;

16.4.1.2. Conduct exit interviews that include a discussion of college-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 college;

16.4.1.3. Retrieve all security-related, college information system-related property;

16.4.1.4. Retain access to college information and information systems formerly controlled by the terminated individual; and

16.4.1.5. Notify college-defined personnel within a college-defined time period.

16.4.2. LIT must establish procedures to sufficiently accommodate reasonably expected scenarios in which the controls in 16.4.1 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.

16.5. Personnel Transfer (Authority - DIR CC: PS-5)

16.5.1. LIT must:

16.5.1.1. 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 college;

16.5.1.2. Initiate transfer or reassignment actions within a college-defined time period following the formal transfer action;

16.5.1.3. Modify access authorizations as needed to correspond with any changes in operational need because of reassignment or transfer; and

16.5.1.4. Notify college-defined personnel or roles within a college-defined time period.

16.6. Access Agreements (Authority - DIR CC: PS-6)

16.6.1. LIT must:

16.6.1.1. Develop and document access agreements for college information systems;

16.6.1.2. Review and update the access agreements at a college-defined frequency; and

16.6.1.3. Verify that individuals requiring access to college information and information systems:

16.6.1.4. Sign appropriate access agreements prior to being granted access; and

16.6.1.5. Re-sign access agreements to maintain access to college information systems when access agreements have been updated or at a college-defined frequency.

16.7. External Personnel Security (Authority - DIR CC: PS-7)

16.7.1. LIT must:

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

16.7.1.2. Require external providers to comply with personnel security policies and procedures established by the college;

16.7.1.3. Document personnel security requirements;

16.7.1.4. Require external providers to notify college-defined personnel or roles of any personnel transfers or terminations of external personnel who possess college credentials and/or badges, or who have information system privileges within a college-defined time period; and

16.7.1.5. Monitor provider compliance with personnel security requirements.

16.8. Personnel Sanctions (Authority - DIR CC: PS-8)

16.8.1. LIT must:

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

16.8.1.2. Notify college-defined personnel or roles within college-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

16.9. Position Descriptions (Authority - DIR CC: PS-9)

16.9.1. LIT must incorporate security roles and responsibilities into college position descriptions.

17. RISK ASSESSMENT

17.1. Procedures (Authority - DIR CC: RA-1)

17.1.1. LIT must:

17.1.1.1. Develop procedures to facilitate the implementation of the Risk Assessment policy and associated controls;

17.1.1.2. Review and update Risk Assessment procedures at a college-defined frequency; and

17.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college Risk Assessment procedures related to the controls in this policy.

17.2. Security Categorization (Authority - DIR CC: RA-2, TAC 202.75, TAC 202.1)

17.2.1. The college's ISO must establish requirements for security categorization of information systems.

17.2.2. LIT must:

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

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

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

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

17.3. Risk Assessment & Supply Chain Risk Assessment (Authority - DIR CC: RA-3, RA-3(1); TAC 202.75, TAC 202.77; TGC 2054.0593)

17.3.1. LIT must:

17.3.1.1. Conduct an assessment of risk, including:

17.3.1.1.1. 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;

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

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

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

17.3.1.3. Review and document risk assessment results in a report on a recurring, college-defined frequency;

17.3.1.4. Disseminate risk assessment results to college-defined personnel or roles;

17.3.1.5. Update the risk assessment at a college-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

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

17.3.1.6.1. At least biennially for systems containing confidential data;

17.3.1.6.2. Periodically, at a frequency determined by the college, for systems containing non-confidential data; and

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

17.3.2. LIT must:

17.3.2.1. Assess supply chain risks associated with college-defined systems, system components, and system services; and

17.3.2.2. Update the supply chain risk assessment at a college-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.

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

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

17.3.2.3.2. LIT's President for all systems identified with a high residual risk.

17.4. Vulnerability Monitoring and Scanning & Update Vulnerabilities to be Scanned (Authority - DIR CC: RA-5, RA-5(2))

17.4.1. LIT must:

17.4.1.1. Monitor and scan for vulnerabilities in each information system and its hosted applications on a recurring frequency, at least annually, in accordance with the college's established process and when new vulnerabilities potentially affecting systems or applications are identified and reported;

17.4.1.2. Employ vulnerability monitoring and scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using college-defined standards for:

17.4.1.2.1. Enumerating platforms, software flaws, and improper configurations;

17.4.1.2.2. Formatting checklists and test procedures; and

17.4.1.2.3. Measuring vulnerability impact;

17.4.1.3. Analyze vulnerability scan reports from vulnerability monitoring activities and results from security assessments;

17.4.1.4. Remediate legitimate vulnerabilities in a college-defined response time in accordance with a college assessment of risk;

17.4.1.5. Share information obtained from the vulnerability scanning and monitoring processes and security assessments with appropriate information system custodians in accordance with the college's internal dissemination procedures; and

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

17.4.2. LIT must update the information system vulnerabilities to be scanned when at least one of the following conditions are met:

17.4.2.1. At a college-defined frequency;

17.4.2.2. Prior to a new scan; and/or

17.4.2.3. When new vulnerabilities are identified and reported.

17.5. Public Disclosure Program (Authority - DIR CC: RA-5(11))

17.5.1. LIT must establish a public reporting channel for receiving reports of vulnerabilities in college information systems and information system components.

17.6. Risk Response (Authority - DIR CC: RA-7)

17.6.1. LIT must respond to findings from security assessments, monitoring, and audits in accordance with college risk tolerance.

18. SYSTEM AND SERVICES ACQUISITION

18.1. Procedures (Authority - DIR CC: SI-1)

18.1.1. LIT must:

18.1.1.1. Develop procedures to facilitate the implementation of the Systems and Services Acquisition policy and associated controls;

18.1.1.2. Review and update System and Information Integrity procedures at a college-defined frequency; and

18.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college System and Services Acquisition procedures related to the controls in this policy.

18.2. Allocation of Resources (Authority - DIR CC: SA-2)

18.2.1. LIT must:

18.2.1.1. Determine high-level information security requirements for each information system or information system service in mission and business process planning;

18.2.1.2. 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

18.2.1.3. Establish a discrete line item for information security in college programming and budgeting documentation.

18.3. System Development Life Cycle (Authority - DIR CC: SA-3)

18.3.1. LIT must:

18.3.1.1. Acquire, develop, and manage information systems using a college-defined system development life cycle that incorporates information security considerations;

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

18.3.1.3. Identify individuals having information security roles and responsibilities; and

18.3.1.4. Integrate the college information security risk management process into system development life cycle activities.

18.3.2. LIT must include information security, security testing, and audit controls in all phases of the system development lifecycle or acquisition process.

18.4. Acquisition Process (Authority - DIR CC: SA-4, TGC §2054.138)

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

18.4.1.1. Security functional requirements;

18.4.1.2. Strength of mechanism requirements;

18.4.1.3. Security assurance requirements;

18.4.1.4. Controls needed to satisfy the security requirements;

18.4.1.5. Security-related documentation requirements;

18.4.1.6. Requirements for protecting security-related documentation;

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

18.4.1.8. Allocation of responsibility or identification of parties responsible for information security and supply chain risk management; and

18.4.1.9. Acceptance criteria.

18.4.2. LIT, when entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for LIT shall include, within or as an addendum to the contract, the “Information Security and Accessibility Standards” Exhibit from the TSUS Contract Management Handbook or, if superseded, the appropriate addendum replacing the exhibit.

18.5. System Documentation (Authority - DIR CC: SA-5)

18.5.1. LIT must:

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

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

18.5.1.1.2. Effective use and maintenance of security functions/mechanisms; and

18.5.1.1.3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

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

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

18.5.1.4. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

18.5.1.5. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

18.5.1.6. Document attempts to obtain information system, information system component, or information system service documentation when such documentation is either unavailable or non-existent and take college-defined actions in response;

18.5.1.7. Protect documentation as required, in accordance with the college risk management strategy; and

18.5.1.8. Distribute documentation to college-defined personnel or roles.

18.6. Security Engineering Principles (Authority - DIR CC: SA-8)

18.6.1. LIT must:

18.6.1.1. Define and establish college security engineering principles; and

18.6.1.2. Apply the security engineering principles in the specification, design, development, implementation, and modification of the information system and information system components.

18.7. External System Services (Authority - DIR CC: SA-9)

18.7.1. LIT must:

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

18.7.1.2. Define and document college oversight and user roles and responsibilities with regard to external information system services; and

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

18.8. Developer Configuration Management (Authority - DIR CC: SA-10)

18.8.1. LIT must require the developer of each information system, information system component, or information system service to:

18.8.1.1. Perform configuration management during at least one of the following life cycle stages: design, development, implementation, operation, or disposal;

18.8.1.2. Document, manage, and control the integrity of changes to college-defined configuration items under configuration management;

18.8.1.3. Implement only college-approved changes to the information system, information system component, or information system service;

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

18.8.1.5. Track security flaws and flaw resolution within the information system, information system component, or information system service and report findings to college-defined personnel.

18.8.2. LIT must require that:

18.8.2.1. The information owner approve all security-related information resources changes for their respective information system(s) through a change control process; and

18.8.2.2. The approval of such changes to occur prior to the implementation of the security-related information resources changes by the college or independent contractors.

18.9. Developer Testing and Evaluation (Authority - DIR CC: SA-11)

18.9.1. LIT must require the developer of the information system, information system component, or information system service, at all post-design stages of the system development life cycle, to:

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

18.9.1.2. Perform the appropriate level and frequency of testing and evaluation based on the classification of data and the security categorization of the information system;

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

18.9.1.4. Implement a verifiable flaw remediation process; and

18.9.1.5. Correct flaws identified during testing and evaluation.

18.10. Unsupported System Components (Authority - DIR CC: SA-22)

18.10.1. LIT must:

18.10.1.1. Replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

18.10.1.2. Provide alternative sources for continued support for unsupported components (e.g., support from external providers, in-house support if technically feasible).

19. SYSTEM AND COMMUNICATIONS PROTECTION

19.1. Procedures (Authority - DIR CC: SC-1)

19.1.1. LIT must:

19.1.1.1. Develop procedures to facilitate the implementation of the System and Communications Protection policy and associated controls;

19.1.1.2. Review and update System and Communications Protection procedures at a college-defined frequency; and

19.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college System and Communications Protection procedures related to the controls in this policy.

19.2. Denial of Service Protection (Authority - DIR CC: SC-5)

19.2.1. LIT must protect information systems against, or limit the effects of, college-defined types of denial-of-service attacks by employing college-defined safeguards.

19.3. Boundary Protection (Authority - DIR CC: SC-7)

19.3.1. LIT must:

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

19.3.1.2. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal college networks; and

19.3.1.3. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with a college security architecture.

19.3.1.4. The President (or their designated representative) and the 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:

19.3.1.4.1. Demilitarized Zone(s) (DMZ);

19.3.1.4.2. Firewall(s);

19.3.1.4.3. Intrusion detection system(s);

19.3.1.4.4. Intrusion prevention system(s); and

19.3.1.4.5. Router(s).

19.4. Transmission Confidentiality and Integrity (Authority - DIR CC: SC-8)

19.4.1. LIT must ensure that each information system protects the confidentiality and/or integrity of transmitted information.

19.4.2. LIT must:

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

19.4.2.2. 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).

19.5. Cryptographic Key Establishment and Management (Authority - DIR CC: SC-12)

19.5.1. LIT must establish and manage cryptographic keys for required cryptography employed within each information system in accordance with college-defined requirements for key generation, distribution, storage, access, and destruction.

19.6. Cryptographic Protection (Authority - DIR CC: SC-13)

19.6.1. LIT must:

19.6.1.1. Determine college-defined cryptographic uses; and

19.6.1.2. Implement college-defined types of cryptography required for each specified cryptographic use.

19.7. Collaborative Computing Devices and Applications (Authority - DIR CC: SC-15)

19.7.1. LIT must:

19.7.1.1. Prohibit remote activation of collaborative computing devices and applications except for college-defined devices and applications; and

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

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

19.8.1. LIT must ensure that each information system that provides name resolution services:

19.8.1.1. 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

19.8.1.2. 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.

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

19.9.1. LIT 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.

19.10. Architecture and Provisioning for Name / Address Resolution Service (Authority - DIR CC: SC-22)

19.10.1. LIT must ensure that information systems that collectively provide name/address resolution service for a component college are fault-tolerant and implement internal and external role separation.

19.11. Protection of Information at Rest (Authority - TSUS ISO Council: SC-28)

19.11.1. LIT must protect the confidentiality and/or integrity of college-defined types of information at rest.

19.11.2. LIT must:

19.11.2.1. Document in a Standard, based on college 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;

19.11.2.2. 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;

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

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

19.11.2.5. Endpoint computing devices not owned by a state agency;

19.11.2.6. Portable computing devices (regardless of ownership); or

19.11.2.7. Removable media (regardless of ownership).

19.12. Process Isolation (Authority - DIR CC: SC-39)

19.12.1. LIT must ensure that each information system maintains a separate execution domain for each executing process.

20. SYSTEM AND INFORMATION INTEGRITY

20.1. Procedures (Authority - DIR CC: SI-1)

20.1.1. LIT must:

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

20.1.1.2. Review and update System and Information Integrity procedures at a college-defined frequency; and

20.1.1.3. Designate an individual as responsible for managing, developing, documenting, and disseminating college System and Information Integrity procedures related to the controls in this policy

20.2. Flaw Remediation (Authority - DIR CC: SI-2)

20.2.1. LIT must:

20.2.1.1. Identify, report to college personnel or roles with information security responsibilities, and correct information system flaws;

20.2.1.2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

20.2.1.3. Install security-relevant software and firmware updates within a college-defined time period of the release of the updates; and

20.2.1.4. Incorporate flaw remediation into the college configuration management process.

20.3. Malicious Code Protection (Authority - DIR CC: SI-3)

20.3.1. LIT must:

20.3.1.1. 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;

20.3.1.2. Automatically update malicious code protection mechanisms as new releases are available in accordance with college configuration management policy and procedures;

20.3.1.3. Configure malicious code protection mechanisms to:

20.3.1.4. Perform periodic scans of information systems at a college-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 college security policy; and

20.3.1.5. Perform one or more of the following in response to malicious code detection: block malicious code; quarantine malicious code; send an alert to college-defined personnel or roles; and/or perform another college-defined action.

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

20.4. Information System Monitoring (Authority - DIR CC: SI-4)

20.4.1. LIT must:

20.4.1.1. Monitor each information system to detect:

20.4.1.2. Attacks and indicators of potential attacks in accordance with college-defined monitoring objectives; and

20.4.1.3. Unauthorized local, network, and remote connections;

20.4.1.4. Identify unauthorized use of information systems through college-defined techniques and methods;

20.4.1.5. Deploy monitoring devices and/or invoke internal monitoring capabilities:

20.4.1.6. Strategically within information systems to collect college-defined essential information; and

20.4.1.7. At ad hoc locations within information systems to track specific types of transactions of interest to the college;

20.4.1.8. Analyze detected events and anomalies;

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

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

20.4.1.11. Obtain legal opinion regarding information system monitoring activities; and

20.4.1.12. Provide college-defined information system monitoring information to college-defined personnel or roles as needed and/or at a college-defined frequency.

20.5. Security Alerts, Advisories, and Directives (Authority - DIR CC: SI-5)

20.5.1. LIT must:

20.5.1.1. Receive information system security alerts, advisories, and directives from college-defined external organizations on an ongoing basis;

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

20.5.1.3. Disseminate security alerts, advisories, and directives to college-defined personnel or roles, college-defined elements within the college, and/or college-defined external organizations; and

20.5.1.4. 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.

20.6. Information Input Validation (Authority - DIR CC: SI-10)

20.6.1. LIT must ensure that each information system checks the validity of college-defined information inputs.

20.7. Information Management and Retention (Authority - DIR CC: SI-12)

20.7.1. LIT 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.

21. SUPPLY CHAIN RISK MANAGEMENT

21.1. Procedures (Authority - DIR CC: SR-1)

21.1.1. LIT must:

21.1.1.1. Develop procedures to facilitate the implementation of the Supply Chain Risk Management policy and associated controls;

21.1.1.2. Review and update Supply Chain Risk Management procedures at a college-defined frequency; and

21.1.1.3. Designate a college-defined individual as responsible for managing, developing, documenting, and disseminating college Supply Chain Risk Management procedures related to the controls in this policy.

21.2. Supply Chain Risk Management Plan (Authority - DIR CC: SR-2)

21.2.1. LIT must:

21.2.1.1. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of college-defined information systems, system components or system services;

21.2.1.2. Implement the supply chain risk management plan consistently across the college; and

21.2.1.3. Review and update the supply chain risk management plan at a college-defined frequency or as required, to address threat, organizational or environmental changes.

21.3. Supply Chain Controls and Processes (Authority - DIR CC: SR-3)

21.3.1. LIT must:

21.3.1.1. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of college-defined information systems or information system components in coordination with college-defined personnel or roles;

21.3.1.2. Employ college-defined supply chain controls to protect against supply chain risks to information systems, information system components, or information system services and to limit the harm or consequences from supply chain-related events; and

21.3.1.3. Document the selected and implemented supply chain processes and controls in security plans, supply chain risk management plan(s), and/or college-defined documents.

21.4. Acquisition Strategies, Tools, and Methods (Authority - DIR CC: SR-5)

21.4.1. LIT must employ college-defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

21.5. Notification Agreements (Authority - DIR CC: SR-8)

21.5.1. LIT must establish agreements and procedures with entities involved in the supply chain for information systems, information system components, or information system services for the one or more of the following:

21.5.1.1. Notification of supply chain compromises;

21.5.1.2. Results of assessments or audits; and/or

21.5.1.3. Institute-defined information and controls.

21.6. Component Disposal (Authority - DIR CC: SR-12)

21.6.1. LIT must dispose of college-defined data, documentation, tools, and/or information system components using college-defined techniques and methods

22. EXCEPTIONS

Pursuant to TAC 202.71(c), the LIT Information Security Officer, with the approval of the college President, may issue exceptions to information security requirements or controls in this policy. Any such exceptions shall be justified, documented, and communicated.

Related Procedures:

Relevant Forms/Documents:

Relevant TSUS Policies/Forms/Documents: Texas DIR Security Control Standards Catalog, LIT.3.01 Information Resources Management, LIT.3.02 Appropriate Use of Information Resources, LIT.3.04 Information Security Program, LIT.3.06 Use of Cloud Services

Relevant Statutes: Texas Administrative Code §202.76

Relevant SACSCOC Standards:

Document History:
Adopted:
Reviewed:
Revised: September 2025