LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology
AREA: Information Technology Area Number: 10.01.01

SUBJECT: Information Systems Management Policy

I. PURPOSE

Lamar University users need timely and secure access to services that provide data and functionality. The purpose of the information systems management policy is to provide appropriate controls to protect the full life cycle of information and applications stored and operated on university information systems or contracted services and to minimize risks during the configuration and management of said systems.

This policy document and the associated Lamar University Technical Control Index (LTCI) incorporate mandated minimum controls from the Texas Control Standards Catalog (TCSC) v2.1 and Texas Administrative Code (TAC) §202.76.a and §202.76.b applicable to information systems management, including but not limited to servers, networks, cloud services, and endpoints. Where appropriate, the policy also adopts more stringent standards as permitted by TAC §202.76.e.

TCSC controls are a combination of strategic (administrative) and tactical (prescriptive technical) controls. To make enforcement easier, this policy document groups strategic controls and provides the rules for the development of applicable procedures and processes by the information owners and custodians. The LTCI groups the associated tactical controls. The same tactical control is written in multiple applicable areas: applications, networks, location, and endpoint. In most cases, technical controls and any applicable standards can be centrally enforced and audited for compliance. Custodians are encouraged to use centrally managed tools to avoid repetition, increase consistency of operation, and ensure compliance.

The language used in this policy follows the Texas State University Systems (TSUS) policy templates and is modified for organization-specific content, where applicable.

Unless otherwise specified, custodians are generally responsible for the development and maintenance of procedures that address the enforcement of controls listed in this policy and the Lamar Technical Control Index. The procedures must be reviewed every three years, at minimum.

Both documents reference the control numbers from TCSC for ease of reference, e.g. [AC-2].

II. SCOPE

This policy applies to all people, departments, and organizations that purchase, develop, manage, or utilize information systems owned, supplied, or used on behalf of Lamar University, regardless of the source of funds or supplier.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A. IDENTIFICATION AND AUTHENTICATION

1. *Identification and Authentication (Organizational Users) [IA-2]*
   1.1. The information owners are responsible for identifying the combination of Personally Identifiable Information (PII), defined under the Texas Business and Commerce Code, as the information required to uniquely identify users and to establish unique electronic identifiers.
   1.2. Custodians must ensure that information systems uniquely identify and authenticate organizational users or processes acting on behalf of organizational users prior to granting the user or process access to a given information system.
      1.2.1. Non-unique identifiers may only be used in situations in which risk analysis, performed by the office of the ISO, demonstrates no need for individual accountability of users.
   1.3. The Information Technology (IT) division is responsible for the generation and distribution of centrally managed, unique electronic identifiers for organizational users, for example, LEA usernames. While it is feasible to generate identifiers, departments are required to utilize the identifiers centrally issued by the IT Division in their information systems to ensure simplicity for users, consistency of authentication, and accountability in audit processes.

2. *Multifactor Authentication To Privileged Accounts [IA-2(1)]*
   2.1. Custodians must implement multifactor authentication for access to privileged accounts on organizational information systems.

3. *Multifactor Authentication To Non-Privileged Accounts [IA-2(2)]*
   3.1. Custodians must implement multifactor authentication for access to non-privileged accounts on organizational information systems.

4. *Device Identification and Authentication [IA-3*]
   4.1. Organization-owned information systems that house or process confidential or regulated information must be uniquely identified and authenticated as defined in the Lamar University Technical Control Index, before establishing a network connection.

5. *Identifier Management [IA-4]*
   5.1. Custodians that manage identifiers, for example, Usernames, MAC Addresses, IP Addresses, and Device Tokens, must:
      5.1.1. Receive authorization from the information owner to assign an identifier to individuals, groups, roles, services, or devices.
      5.1.2. Develop, document, and maintain a naming convention of identifiers for individuals, groups, roles, or devices.
      5.1.3. Select an identifier that identifies an individual, group, role, or device.
      5.1.4. Assign the identifier to the intended individual, group, role, or device.
      5.1.5. Prevent reuse of identifiers.
   5.2. Custodians must ensure a user's access authorization is appropriately modified or removed when the user's employment, job responsibilities, or affiliation with the organization changes.

6. *Authenticator Management and [IA-5]*

6.1. Custodians, during initial authenticator setup, for example, Passwords, Passphrases, and Tokens must:
  6.1.1. Include procedures to verify the identity of the individual, group, role, or device receiving the authenticator. For example, identity verification steps can include verifying a portion of PII, email validation, Mac Address, or IP Address.
  6.1.2. Ensure that the authenticator generated complies with the complexity requirements specified in the Security Passwords Standard.
6.2. Custodians must establish and implement administrative procedures for:
  6.2.1. Establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators.
  6.2.2. Changing authenticators for group/role accounts when membership of those accounts changes.
  6.2.3. Changing default authenticators prior to first use.
  6.2.4. Ensure that the minimum and maximum lifetime restrictions and reuse conditions comply with the requirements specified in the Security Passwords Standard.
  6.2.5. Changing or refreshing authenticators comply with the requirements specified in the Security Passwords Standard.
  6.2.6. Protecting authenticator content from unauthorized disclosure and modification
  6.2.7. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators. For example, maintaining possession of individual authenticators, not loaning, or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately.
  6.2.8. Changing authenticators for group or role accounts when membership to those accounts changes.
6.3. Custodians must configure information systems to enforce:
  6.3.1. The change of default authenticator content during system installation.
  6.3.2. The level of authenticator complexity so that it complies with the Security Passwords Standard.
  6.3.3. The use of Cryptographic protection for the storing and transmission of authenticators. For example, passwords must be stored utilizing a non-reversible Hashing Algorithm such as SHA512 with salt and utilizing TLS1.2 encryption for transmission.

7. *Password Based Authentication [IA-5(1)]*
7.1. Custodians, for password-based authentication, must:
  7.1.1. Maintain a list of commonly used, expected, or compromised passwords and update the list at minimum, annually and when organizational passwords are suspected to have been compromised directly or indirectly,
  7.1.2. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords, maintained by the Office of the Information Security Officer (ISO).
  7.1.3. Transmit passwords only over cryptographically protected channels.
  7.1.4. Store passwords using an approved salted key derivation function, preferably using a keyed hash.
  7.1.5. Require immediate selection of a new password upon account recovery.
  7.1.6. Allow user selection of long passwords and passphrases, including spaces and all printable characters.
  7.1.7. Employ automated tools to assist the user in selecting strong password authenticators.
  7.1.8. Enforce password composition and complexity rules as specified in the Password Standard.

8. *Authenticator Feedback [IA-6]*
   8.1. Custodians must ensure that information systems obscure feedback of authentication information entered during authentication processes.
   8.2. Refer to the LTCI for specified information system configuration**.**

9. *Cryptographic Module Authentication [IA-7]*
   9.1. Implement mechanisms for authentication to cryptographic modules in information systems.
   9.2. Ensure that implemented cryptographic modules meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.
   9.3. Refer to the LTCI for specified information system configuration**.**

10. *Identification and Authentication (Non-Organizational Users) [IA-8]*
    10.1. The information system must uniquely identify and authenticate non-organizational users or processes acting on behalf of a non-organizational user.
    10.2. In most circumstances, the identification requirements for a non-organizational user must be treated similarly to an organizational user. An electronic identifier must be generated for the non-organizational user. All authentication, authorization, and access requirements for the organizational user will then apply to the non-organizational user.
    10.3. The information owner, in consultation with the Office of the ISO, can authorize the use of an external identifier and authentication provider per information system. The Office of the ISO will authorize the custodian to implement controls that utilize security attributes of the non-organizational user from the external identity source. The custodian must implement service identification and authentication control [IA-9].
       10.3.1. Refer to the LTCI for specified information system configuration.

11. Re-Authentication [IA-11]
    11.1. Ensure that the circumstances or situations requiring users to re-authenticate on an information system comply with the requirements specified in the Reauthentication Standard.

B. ACCESS CONTROL

1. *Account Management [AC-2]*
   1.1. For each information system, the information owner, working in conjunction with the custodian, the Office of the ISO, and the Information Resource Manager (IRM), either through manual or automated mechanisms, must:
      1.1.1. Assume the role of the account manager.
      1.1.2. Define and document, the types of information system accounts that support organizational missions and business functions.
      1.1.3. Specify the authorized users of an information system, group and role membership, access authorization, and other attributes for each account.
      1.1.4. Authorize access to information systems based on:
         1.1.4.1. A valid access authorization.
         1.1.4.2. Intended system usage.
         1.1.4.3. Other attributes required by mission or business function. Examples of other attributes can be restrictions on time of day, days of the week, and point of origin.
      1.1.5. Establish processes and procedures for re-issuing accounts that are using shared credentials (if used) when individuals are no longer authorized.
      1.1.6. Assume responsibilities defined under TAC 202.72.1 and the Lamar Information Security Program.
      1.1.7. Authorize remote access to the information system and document the authorization in the security plan.
      1.1.8. Authorize wireless access to the information system and document the

authorization in the security plan.

1.1.9. Authorize mobile device access to the information system and document the authorization in the security plan.

1.2. For each information system, the custodian working, in conjunction with the information owner and the Office of the ISO, either through manual or automated mechanisms must:

1.2.1. Identify and select the types of information system accounts. For example, the types of accounts could include, Individual, Group, Privileged, Guest, Emergency, Developer, Vendor, Temporary, and Service.

1.2.2. Establish and document appropriate naming conventions and management cycles for each account type.

1.2.3. Establish conditions for group and role membership.

1.2.4. Establish and implement processes for changing shared/group account credentials (if deployed) when individuals are removed from a group in consultation with respective information owners.

1.2.5. Require approval from the information owner to create information system accounts.

1.2.6. Create, enable, modify, disable, and remove information system accounts in accordance with information owner-defined procedures and conditions, such as valid access authorization.

1.2.7. Notify the Office of the ISO and the IRM of the creation, modification, enabling, disabling, and removal actions for very highly privileged accounts.

1.2.8. Monitor the use of information system accounts for atypical usage. Examples of atypical usage can include access at times of the day and from locations that are not consistent with normal usage patterns.

1.2.9. Notify the Office of the ISO when atypical usage of information system accounts occurs.

1.2.10. Notify the information owner, within 30 calendar days, when:

1.2.10.1. Accounts are no longer required.

1.2.10.2. Users are terminated or transferred.

1.2.10.3. Individual system usage or need-to-know changes.

1.2.11. Review accounts for compliance with account management requirements at least once every two years.

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

1.2.13. Configure the information system to log out users after 900 seconds of inactivity (idle time).

1.2.14. Disable accounts of users posing a significant risk immediately upon the discovery of the risk. For example, a significant risk to the organization can be a compromised account.

1.2.15. Notify the Office of the ISO of user accounts posing a significant risk to the organization upon the discovery of the risk.

1.2.16. Additionally, manage information systems in accordance with the responsibilities defined under TAC 202.72.2 and the Lamar Information Security Program.

1.2.17. Develop, maintain, and implement procedures for information system maintenance controls.

2. *Disable Accounts [AC-2(3)]*

2.1. Disable accounts within 30 Calendar days when the accounts:

2.1.1. Have expired.

2.1.2. Are no longer associated with a user or individual.

2.1.3. Are in violation of organizational policy.

2.1.4. Have been inactive for at least 6 months.

3. *Access Enforcement [AC-3]*

3.1. Custodians must ensure that information systems enforce approved authorizations for logical access to information and system resources.
3.1.1. Refer to the LTCI for specified information system configuration.

4. *Separation of Duties [AC-5]*
4.1. Separation of duties addresses the potential abuse of authorized privileges and assists in reducing the risk of malevolent activities. The information owner is responsible for:
4.1.1. Identifying and documenting duties of individuals requiring separation.
4.1.2. Defining information system access authorization to support the separation of duties.

5. *Least Privilege [AC-6]*
5.1. The principle of least privilege ensures that users, and processes acting on behalf of the user, operate at privilege levels no higher than necessary to accomplish mission or business functions. The information owners must incorporate the principle prior to authorizing access.
5.2. The information owners must establish processes and procedures to explicitly authorize access to security functions, which includes any network-based privilege access. (Principles of Least Access).
5.3. Privileged accounts on the information system, for example, accounts with local administrative privileges on the information system, must be restricted to the designated custodian for that information system. (Principles of Least Access).
5.4. Custodians must select and enforce the least privileged roles when enforcing access control within the information system.
5.5. Custodians who operate on information systems with privileged access must use an account with the least privilege necessary to complete administrative activities. For example, use Server Operator (SO) in lieu of Domain Administrator (DA).
5.6. Users must use an unprivileged account when using information systems. Users that have privileged and unprivileged accounts must default to using unprivileged accounts, particularly when accessing untrusted networks such as the Internet.
While it is convenient to continuously maintain privileged access for installing software directly from the Internet, this provides a backdoor or weakness for malware to exploit and self-install without the user's knowledge or intervention. Hence, the privileged account must be restricted to privileged activities.

6. *Unsuccessful Logon Attempts [AC-7]*
6.1. Custodians must ensure that each information system:
6.1.1. Enforces a limit of 5 consecutive invalid logon attempts by a user or source of authentication during a 30-minute period of time.
6.1.2. Automatically performs at least one of the following actions when the maximum number of unsuccessful attempts is exceeded:
6.1.2.1. Locks the account or node for 30 minutes.
6.1.2.2. Locks the account or node until released by an administrator.
6.1.2.3. Delays the next logon prompt by 2 seconds.
6.1.2.4. Notifies the information custodian.
6.1.3. Refer to the LTCI for specified information system configuration.

7. *System Use Notification [AC-8]*
7.1. Custodians must ensure that each information system:
7.1.1. Displays to human users at logon interfaces a Lamar University-defined system use notification 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:

7.1.1.1. Users are accessing an organizational information system.
7.1.1.2. Information system usage may be monitored, recorded, and subject to audit.
7.1.1.3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
7.1.1.4. Use of the information system indicates consent to monitoring and recording.

7.2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
7.3. For publicly accessible information systems that do not have login interfaces:
7.3.1. Displays system use information under Lamar University approved banners before granting further access.
7.3.2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
7.3.3. Includes a description of the authorized uses of the system.
7.4. Refer to the LTCI for specified information system configuration.

8. *Permitted Actions without Identification or Authentication [AC-14]*
8.1. When the information system or portions of the information system functionality permit user actions without the need for identification or authentication, such functionality and its rationale must be identified and documented in the Security Plan for the information system.
8.2. When circumstances require the need to bypass identification or authentication for the information system, the Office of the ISO must be informed of the rationale.

9. *Remote Access [AC-17]*
9.1. Remote access to Lamar University networks and Lamar University-owned information processing facilities must be accomplished over an encrypted Virtual Private Network (VPN), as defined and specified by the Office of the ISO.
9.2. Custodians must restrict privileged access to information processing facilities by routing all access through managed access points, for example, Jump boxes, Bastion hosts, etc.

10. *Wireless Access [AC-18]*
10.1. Wireless networks must be configured based on the connection requirements provided in the Lamar University Technical Control Index.
10.2. Custodians must disable the wireless networking capabilities of information systems prior to deployment if wireless networking is not used. For example, if a printer is connected by wire, the embedded wireless interface must be disabled before deployment.

11. *Access Control for Mobile Devices [AC-19]*
11.1. Custodians must configure university-owned mobile devices to employ container encryption to protect the confidentiality and integrity of information. For example, Mobile Device Management/Mobile Access Management (MDM/MAM) policies can be configured to manage endpoints such as laptops, tablets, and smartphones that take advantage of the built-in capabilities of the platform.

12. *Use of External Information Systems [AC-20]*
12.1. The university 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:
12.1.1. Access the information system from external information systems.
12.1.2. Process, store, or transmit institution-controlled information using external

information systems.

13. *Publicly Accessible Content [AC-22]*
    13.1. The Office of Marketing Communications coordinates and publishes publicly accessible information to information systems, such as the university's main website. The department must train authorized individuals to ensure that publicly accessible information does not contain confidential, sensitive, or regulated information. The department must establish processes to review the content of information prior to publishing. This review is to ensure nonpublic information is not published. The department will continuously review the content on publicly accessible information systems at least monthly for confidential, sensitive, or regulated information, remove such information if discovered, and notify the Office of the ISO.

C. AUDIT AND ACCOUNTABILITY

1. *Event Logging [AU-2]*
    1.1. Information System Owners must:
        1.1.1. Document a standard defining the types of events that each information system is capable of logging, including the frequency at which the types of events selected for logging are reviewed and updated.
        1.1.2. 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 Auditable Events and Log Content Standard.
    1.2. Custodians must:
        1.2.1. 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.
        1.2.2. 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.
        1.2.3. 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.

2. *Content of Audit Records [AU-3]*
    2.1. Custodians must ensure that Audit records contain the following:
        2.1.1. What type of event occurred.
        2.1.2. When the event occurred.
        2.1.3. Where the event occurred.
        2.1.4. Source of the event.
        2.1.5. Outcome of the event.
        2.1.6. Identity of any individuals, subjects, or objects/entities associated with the event.

3. *Audit Log Storage Capacity [AU-4]*
    3.1. Custodians must allocate audit storage capacity on the information system to store 14 days of audit data.

4. *Response to Audit Logging Process Failures [AU-5]*
    4.1. Custodians must:
        4.1.1. 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.
    4.2. 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.

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

4.3. Refer to the LTCI for specified information system configuration.

5. *Audit Record Review, Analysis, and Reporting [AU-6]*

5.1. Custodians are responsible for reviewing and analyzing information system audit records (audit logs) at a frequency identified in the LTCI.

5.2. Custodians must identify and report inappropriate activities, unusual activity, or actionable findings to the Office of the ISO.

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

6. *Time stamps [AU-8]*

6.1. Custodians must:

6.1.1. Configure each information system to:

6.1.1.1. Use internal system clocks to generate time stamps for audit records.

6.1.1.2. Synchronize internal system clocks with an authoritative source of time specified by Lamar University.

6.1.2. Ensure that audit records record time stamps in milliseconds:

6.1.2.1. Use Coordinated Universal Time.

6.1.2.2. Have a fixed local time offset from Coordinated Universal Time.

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

6.2. Refer to the LTCI for specified information system configuration.

7. *Protection of Audit Information (AU-9*

7.1. Custodians must protect audit information and audit tools from unauthorized access, modification, and deletion.

7.1.1. Refer to the LTCI for specified information system configuration.

8. *Non-Repudiation [AU-10]*

8.1. Custodians must ensure that the information system is configured to protect against an individual (or process acting on behalf of an individual) falsely denying having performed an action. For example, signing of contracts, approving financial transactions, or sending specific information.

8.1.1. Refer to the LTCI for specified information system configuration.

9. *Audit Record Retention [AU-11]*

9.1. Audit records that are no longer needed for administrative, legal, audit, or other operational purposes must be retained for a minimum of 90 days or in accordance with the record retention policy to Support after-the-fact investigations of Incidents.

10. *Audit Record Generation [AU-12]*

10.1. Lamar University information systems must:

10.1.1. Provide audit record generation capability for the auditable events required by this policy and related organizational policies and Auditable Events and Log Content standards.

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

10.1.3. In alignment with this policy and related organizational policies and Auditable Events and Log standards, generate audit records for necessary types of events and ensure the generated records contain sufficient content.

11. *Cross-Organizational Auditing Logging [AU-16]*

11.1. When auditing information is transmitted across organizational boundaries, the

unique organizational identifier, for example, username, must be maintained to allow correlation of events between information systems.

D. MAINTENANCE

1. *Controlled Maintenance [MA-2]*
   1.1. Custodians must perform the following activities to minimize unforeseen failures due to the lack of maintenance:
      1.1.1. Schedule, perform, document, and review records of maintenance, repair, and/or replacement of information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.
      1.1.2. 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.
      1.1.3. Seek explicit approval from the information system owner prior to the removal of information systems or information system components that process SPI or Confidential information from the organizational facilities, for off-site maintenance, repairs, and/or replacement.
      1.1.4. Sanitize equipment to remove all data from associated media, using an approved non-recoverable technique prior to removal from the organizational facilities, for off-site maintenance, repairs, and/or replacement, for example, after receiving a return materials authorization (RMA).
      1.1.5. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair, and/or replacement actions. For example, encryption at rest, management policies, etc.
      1.1.6. Include, at a minimum, the following information in the maintenance records:
         1.1.6.1. Date and time of maintenance.
         1.1.6.2. Name of individuals and/or groups performing the maintenance.
         1.1.6.3. Name of escort, if applicable.
         1.1.6.4. A description of the maintenance performed.
         1.1.6.5. Information system component/equipment removed or replaced (including identification number, if applicable).

2. *Maintenance Tools [MA-3]*
   2.1. In information processing facilities that house and process SPI or other confidential information, custodians must establish procedures to control and monitor information system maintenance tools. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code into a facility either intentionally or unintentionally and subsequently into other information systems.

3. *Nonlocal Maintenance [MA-4]*
   3.1. Custodians must initiate, approve, and monitor any nonlocal maintenance and diagnostic activity. This includes any remote sessions with contracted vendors or service providers.
   3.2. Custodians must allow the use of nonlocal maintenance and diagnostic tools only as consistent with this policy. Tools that alter the security posture of the information system, that exhibit the following characteristics must be used only after notification to the office of the ISO:
      3.2.1. Back door with persistent presence.
      3.2.2. Copying or exfiltration of data.
      3.2.3. Hardcoded credentials.
      3.2.4. Auto-discovery of devices or services.
      3.2.5. Periodic contact to or from external sites.
      3.2.6. Persistent debug mode that captures confidential or sensitive information in logs.
   3.3. Maintenance work conducted over a remote access session should be in accordance

with remote access requirements, as specified in [AC17], above.

3.4. Maintenance work conducted with a tool such as screen shares must utilize strong authenticators, one-time passwords, or one-time use sessions.

3.5. Custodians must maintain records for nonlocal maintenance, and diagnostic activities.

3.6. Custodians must terminate session and network connections when nonlocal maintenance is completed.

4. Maintenance Personnel [MA-5]

4.1. For information processing facilities that house or process confidential information, custodians must:

4.1.1. Establish processes and procedures for authorization of maintenance personnel.

4.1.2. Maintain a list of authorized maintenance organizations and personnel.
In this context, maintenance personnel refer to individuals performing hardware or software maintenance on information systems. Security requirements for personnel who perform maintenance duties that place them within the physical perimeter of the information systems, such as custodial staff and Facilities employees, are covered in the Physical Environmental Policy (PE).

4.1.3. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.

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

5. Timely Maintenance [MA-6]

5.1. Custodians are responsible for maintaining support contracts that ensure maintenance support or spare parts for information systems that house or process confidential information to meet relevant Recovery Time Objectives (RTO).

E. SYSTEM AND INFORMATION INTEGRITY

1. Flaw Remediation [SI-2]

1.1. Custodians are responsible for identifying, planning, and correcting information system flaws. Information system flaws could include announced software and firmware updates, patches, and hotfixes that address security-related vulnerabilities. Additionally, flaws could also include vulnerabilities discovered during security assessment, continuous monitoring, incident response activities, and system error handling.

1.2. When feasible, custodians must test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation

1.3. Custodians must install security-relevant software and firmware updates within 30 calendar days of the release of the update. When the vendor does not have a fix for a security vulnerability, custodians must report the flaw to the Office of the ISO, so compensation controls can be enforced.

1.4. Custodians must follow configuration and change management processes and procedures for flaw remediation.

2. Malicious Code Protection [SI-3]

2.1. Custodians must implement centrally managed signature-based and/or non-signature-based malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
Malicious code includes, for example, viruses, worms, etc. Malicious code protection mechanism examples include anti-virus, endpoint detection, and response (EDR) solutions, etc.

2.2. Custodians must configure malicious code protection mechanisms to automatically update as new releases are available in accordance with institutional configuration

management policy and procedures.

2.3. Custodians must configure the malicious code protection mechanism to:

2.3.1. Perform weekly, full scans of the information system and real-time scans of files at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with this policy.

2.3.2. Audit the detection of any malicious code.

2.3.3. Automatically, block or quarantine malicious code. When neither action is possible, alert the Office of the ISO.

2.4. False positives during malicious code detection and eradication that can potentially impact the availability of the information system must be reported to the Office of the ISO.

3. *Information System Monitoring [SI-4]*

3.1. Custodians must monitor the information system to detect:

3.1.1. Attacks and indicators of potential attacks.

3.1.2. Unauthorized local network and remote connections.

3.2. Custodians must identify the unauthorized use of information systems, utilizing appropriate tools and techniques. Examples of appropriate tools include intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

3.3. Custodians must, upon specific direction from the office of the ISO, deploy monitoring devices and/or invoke internal monitoring capabilities:

3.3.1. Strategically within information systems to collect the information specified in the Auditable Events and Log Content Standard.

3.3.2. At ad hoc locations within information systems to track specific types of transactions of interest to the organization.

3.4. Custodians must analyze detected events and anomalies.

3.5. Custodians must protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

3.6. Custodians must adjust the level of information system monitoring activity whenever there is a change in risk to the university's operations and assets, individuals, or other organizations.

3.7. Custodians must obtain a legal opinion regarding information system monitoring activities in accordance with applicable Federal laws, Executive Orders, Directives, Policies, or Regulations.

3.8. Custodians must provide the information specified in the Auditable Events and Log Content Standard, as directed by the Office of the ISO.

4. *Security Alerts, Advisories, and Directives [SI-5]*

4.1. The Office of the ISO receives security alerts, advisories, and directives from various external agencies such as the Texas Department of Information Resources (DIR), MS-ISAC, REN-ISAC, etc., on an ongoing basis and generates campus security alerts, advisories, and directives to affiliated users as necessary. Custodians are responsible for implementing security directives in accordance with applicable time frames or notifying the Office of the ISO of the degree of non-compliance.

5. *Spam Protection [SI-8]*

5.1. Custodians must employ automatically updated protection mechanisms at information system entry and exit points to detect and prevent unsolicited messages and malware.

6. *Information Input Validation [SI-10]*

6.1. Custodians must ensure that each information system checks the validity of information inputs.

6.1.1. Refer to the LTCI for specified information system configuration.

7. *Information Handling and Retention [SI-12]*

7.1. Custodians are responsible for establishing procedures to manage and retain

information within the information system and information output from the system in accordance with applicable, Federal and state laws, executive orders, and university data retention schedules.

F. MEDIA PROTECTION

1. *Media Access [MP-2]*
   1.1. Information system media includes both digital and non-digital media. Access to information system media that contains confidential or regulated information must be restricted to organizational users or roles.

2. *Media Storage [MP-4]*
   2.1. All information system users are responsible for securely storing digital and non-digital media within physically controlled areas. Examples of physically controlled areas include a locked drawer, desk, cabinet, or controlled media library.
   2.2. Digital media containing confidential or regulated information must implement cryptographic mechanisms as specified in the LTCI, to protect the confidentiality and integrity of the information, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3. *Media Transport [MP-5]*
   3.1. Non-digital media containing confidential or regulated information that leaves controlled areas must be protected by physical safeguards, such as locked storage, during transport.
   3.2. For information system media that contain confidential or regulated information, Custodians must:
      3.2.1. Maintain accountability for the information system media during transport.
      3.2.2. Document activities associated with the transport of information system media.
      3.2.3. Restrict the activities associated with the transport of information system media to authorized personnel.

4. *Media Sanitization, Review, Approve, Track, Document, and Verify [MP-6], [MP-6(1)]*
   4.1. Custodians must review, approve, track, document, and verify media sanitization and disposal actions.
   Media containing confidential or regulated information must be sanitized directly by the university or contractually. Sanitization of media must occur, prior to disposal, release out of university control, or release for re-use. The strength and integrity of the sanitization mechanism employed must be commensurate with the security category or classification of the information.
      4.1.1. Non-digital media that contain confidential or regulated information must be physically destroyed by shredding prior to leaving university premises.
      4.1.2. Equipment with non-removal digital media, such as copiers, scanners, printers, computers, tablets, laptops and phones, network components, etc., must be factory reset and physically destroyed prior to removal from the university.
      4.1.3. Equipment with non-removal digital media, such as network devices, must be factory reset prior to sending them for repairs, to ensure university configurations are erased.
      4.1.4. Equipment with removable digital media, such as computers, laptops, external hard drives, etc., must have the storage media removed and physically destroyed, such that data cannot be reconstituted, prior to disposition from the university.
   4.2. Custodians must follow additional steps for equipment that is under warranty, lease, or contract:
      4.2.1. If equipment has non-removable media that needs to be sent back for repair/RMA, custodians must factory reset before sending the equipment.

4.2.2. Obtain a certificate of data destruction from vendors when equipment is returned at lease end or at equipment end of life.
4.2.3. When financially feasible, procure equipment with removable digital media, like hard drives, such that warranty replacements do not require the media to be sent back to the manufacturer.
4.2.4. If the removal of digital media violates the terms of the warranty, then the custodians must cryptographically erase the digital media prior to the return of equipment to the manufacturer, RMA, or repair.

4.3. Users must physically destroy portable digital media such as CD-ROMs, USB Flash drives, Memory cards, etc. when the media has reached the end of useful life.

4.4. Owners and custodians must:
4.4.1. Destroy electronic records in accordance with Texas Government Code § 441.185 and in compliance with Lamar University's records retention schedule.
4.4.2. Retain, for the duration of the required retention period, a hard copy or other electronic copy of records from data processing equipment at the time of removal if the applicable retention period for the record has not expired.
4.4.3. Consider the incorporation guidelines from Texas DIR regarding the sale or transfer of computers and software into, standards, guidelines, and procedures.
4.4.4. Keep a record or form, in electronic or hard copy, documenting the removal, and completion of sanitization of media that stored confidential and regulated information with the following information:
4.4.4.1. Date.
4.4.4.2. Description of the item(s) and serial number(s).
4.4.4.3. Inventory numbers(s).
4.4.4.4. The process and sanitization tools used to remove the data or method of destruction.
4.4.4.5. The name and address of the organization to which the equipment was transferred.

5. *Media Use [MP-7]*
5.1. Confidential or regulated information must only be stored on digital media that support cryptographic mechanisms as specified in [MP-4] and [MP-5] of the Lamar Technical Control Index.
5.2. The Office of the ISO is responsible for designating the types of media that are prohibited or restricted for use for each data classification type.
5.3. The use of portable storage devices in organizational systems is prohibited when such devices have no identifiable owner.

6. *Media Downgrading [MP-8]*
6.1. Non-digital media, when subject to release outside the organization (downgraded), must be evaluated for data classification. The downgrading process must ensure that confidential or regulated information is removed such that the information cannot be retrieved or reconstituted. Examples of downgrading include but are not limited to redaction, the addition of empty spaces or slack spaces.
6.2. Digital media, when downgrading from storing regulated or confidential information to sensitive or public information, must be cryptographically erased such that the information cannot be retrieved or reconstituted. For example, Hard drives can be overwritten a minimum of three times with random data to ensure that confidential information cannot be retrieved, prior to re-use.

G. SYSTEM AND COMMUNICATION PROTECTION

1. *Denial of Service Protection [SC-5]*
1.1. Custodians must, during all aspects of system design, consider the utilization and capacity of the information system when managing risk from Denial of Service (DOS)

due to malicious attacks.

1.2. Custodians must employ tools to monitor and detect indicators of DOS attacks and monitor information resources to determine if sufficient resources exist to prevent effective DOS attacks.

1.3. Custodians must report any detected DOS, due to a malicious attack, to the Office of the ISO.

2. *Boundary Protection [SC-7]*

2.1. Custodians must, in conjunction with the Office of the ISO:

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

2.1.2. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal institutional networks.

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

2.2. The Office of the ISO, working in conjunction with the information owners and custodians, is authorized to implement safeguards (tools and technologies) to prevent unauthorized exfiltration of information for both secure and insecure protocols.

2.3. Custodians must protect information systems against unauthorized physical connections.

2.4. The President or their designated representative and the office of the ISO 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:

2.4.1. Demilitarized Zone(s) (DMZ).

2.4.2. Firewall(s).

2.4.3. Intrusion detection system(s).

2.4.4. Intrusion prevention system(s).

2.4.5. Router(s).

2.5. Refer to the LTCI for specified information system configuration.

3. *Transmission Confidentiality and Integrity [SC-8]*

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

3.2. Custodians must:

3.2.1. Document in a standard, based on institutional risk-management decisions, encryption requirements for data transmissions of confidential and non-confidential information, and encryption key standards and management.

3.2.2. 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).

3.3. Refer to the LTCI for specified information system configuration**.**

4. *Network Disconnect [SC-10]*

4.1. Custodians must configure the information system to terminate network connection associated with a communications session at the end of the session or after 900 seconds of inactivity.

4.1.1. Refer to the LTCI for specified information system configuration**.**

5. *Cryptographic Key Establishment and Management [SC-12]*

5.1. The Office of the ISO is responsible for acting as the Certificate Authority (CA) for digital certificates for the university. The office is responsible for establishing standards and tools to manage cryptographic keys for required cryptography employed within the information system in accordance with industry best practices and applicable

regulations.

5.2. To maintain the availability of information systems and prevent the loss of data due to lost cryptographic keys, information owners, users, and custodians must follow procedures established by the Office of the ISO.

6. Cryptographic Protection [SC-13]

6.1. Cryptographic use:

6.1.1. Confidential and regulated information that is transmitted over a public network (e.g., the Internet) must be encrypted as described in [SC-8].

6.1.2. Confidential and regulated information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted.

6.1.3. Confidential and regulated information must be encrypted if copied to or stored on a portable computing device, removable media, or a non-state agency-owned computing device.

6.2. Types of cryptography required for each specified cryptographic use.

6.2.1. Refer to the LTCI for specified information system configuration**.**

7. Collaborative Computing Devices and Applications [SC-15]

7.1. Lamar University must:

7.1.1. Prohibit remote activation of collaborative computing devices and applications except for devices and applications identified in the Authorized Software and Devices Collaborative Computing document.

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

8. Public Key Infrastructure Certificates [SC-17]

8.1. Information systems that are publicly accessible and use public-key certificates for securing communications must utilize a certificate compliant with the standards specified by the Office of the ISO and be obtained from an approved certificate service provider.

8.2. Custodians must restrict the use of valid self-signed certificates for the management of information systems, with the limitation that access is restricted to campus network ranges only.

8.3. Vendors who host information systems for the university that do not utilize Lamar network domains must use certificates issued by a public certificate service provider that meets or exceeds standards specified by the Office of the ISO.

9. Secure Name/Address Resolution Service (Authoritative Source [SC-20]

9.1. Custodians must ensure that each information system that provides name resolution services:

9.1.1. 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.

9.1.2. 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.

9.2. Refer to the LTCI for specified information system configuration**.**

10. *Secure Name/Address Resolution Service (Recursive or Caching Resolver [SC-21]*

10.1. Custodians 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.

11. *Architecture and Provisioning for Name/Address Resolution Service [SC-22*]

11.1. Custodians must ensure that information systems that collectively provide name/address resolution service for Lamar University are fault-tolerant and implement internal and external role separation.

12. Fail In Known State [SC-24]

12.1. Custodians must configure information systems to fail secure in the event of a failure, preserving its state information to return to normal mode of operation, unless instructed otherwise by the ISO.

12.1.1. Refer to the LTCI for specified information system configuration.

13. Protection of Information at Rest [SC-28]

13.1. Custodians must protect the confidentiality and integrity of confidential and regulated information at rest by utilizing encryption standards specified in the LTCI.

13.2. Custodians must:

13.2.1. Configure and manage encryption for information storage devices, portable storage devices, removal media, and encryption keys as specified in the LTCI.

13.2.2. Encrypt confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., a web server or file server accessible without authentication or other access controls).

13.2.3. Require that confidential information be encrypted if copied to or stored on the use of portable devices to store confidential information.

13.2.3.1. Endpoint computing devices not owned by a state agency.

13.2.3.2. Portable computing devices (regardless of ownership).

13.2.3.3. Removable media (regardless of ownership).

14. Process Isolation SC-39]

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

H. CONFIGURATION MANAGEMENT

1. Baseline Configuration [CM-2]

1.1. Custodians are responsible for developing, documenting, and maintaining (either manually or by use of automated mechanisms), under configuration management, a current baseline configuration of each information system. Baseline configurations include information about information system components, including standard software packages installed on system components, such as workstations, notebook computers, servers, network components, or mobile devices, current version numbers, patch information on operating systems, applications, and configuration settings/parameters, network topology, and the logical placement of those components within the system architecture. Typically, baseline configurations are captured and maintained in a central Configuration Management Database (CMDB). Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations require creating new baselines as information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

1.2. Custodians, to the extent practical, shall maintain a baseline configuration for information system development and an environment that is managed separately from the production baseline configuration. Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development, incompatibilities, and testing activities.

1.3. Configuration baselines must be captured as part of information system component installation, upgrade, and during changes to information system architecture.

1.4. Custodians are responsible for retaining previous versions of baseline configurations to support rollback as part of the change management processes.

1.5. Working closely with the Office of the ISO on areas determined to be high risk, custodians must enforce enhanced configuration on components or devices. Enhanced configurations may include additional security safeguards for systems. Circumstances that require enhanced configuration may include international travel and return for ITAR compliance.
1.6. Review and update the baseline configuration of each information system:
1.6.1. At least annually
1.6.2. When required due to changes to regulatory requirements and technical architecture.
1.6.3. When information system components are installed or upgraded.

2. *Configuration Change Control [CM-3]*
2.1. Lamar University must:
2.1.1. Determine and document the types of changes to information systems that are configuration-controlled.
2.1.2. Review proposed configuration-controlled changes to information systems and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.
2.1.3. Document configuration change decisions associated with the information systems.
2.1.4. Implement approved configuration-controlled changes to the information systems.
2.1.5. Retain records of configuration-controlled changes to information systems as specified in Lamar University's records retention schedule.
2.1.6. Monitor and review activities associated with configuration-controlled changes to information systems.
2.1.7. Coordinate and provide oversight for configuration change control activities through organization-defined configuration change control elements that convene at an institution-defined frequency and/or when institution-denied configuration change conditions are met.
2.2. Lamar University must ensure that all security-related information resource changes are approved by the information owner (or designee) through a change control process.

3. *Impact Analyses [CM-4]*
3.1. Custodians must analyze changes to each information system to determine potential security impacts prior to change implementation.
3.2. Custodians must ensure that:
3.2.1. All security-related information resource changes are approved by the information system owner through a change control process.
3.2.2. Such approval occurs prior to implementation by the institution or independent contractors.

4. *Access Restrictions for Change [CM-5]*
4.1. Information system owners must define, document, approve, and enforce physical and logical access restrictions associated with changes to each information system.

5. *Configuration Settings [CM-6]*
5.1. Custodians must:
5.1.1. Establish and document configuration settings for information technology products employed within the information system using ISO-recommended security configuration checklists that reflect the most restrictive mode consistent with operational requirements.
5.1.2. Implement the configuration settings.
5.1.3. Identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements.
5.1.4. Monitor and control changes to the configuration settings in accordance with

university policies and procedures.

6. *Least Functionality [CM-7]*
   6.1. During the configuration of the information system, custodians must utilize the principles outlined in the Lamar University Technical Control Index to provide only essential capabilities.
   6.2. Insecure ports and services that are documented in the Lamar University Technical Control Index are prohibited from use in production environments.

7. *Information System Component Inventory [CM-8]*
   7.1. Custodians are responsible for developing, documenting, and maintaining, as part of the baseline, an inventory of information system components that:
      7.1.1. Accurately reflects the current information system.
      7.1.2. Includes all components of the information system within its Authorization Boundary.
      7.1.3. Includes a level of granularity necessary for reporting, tracking, and achieving effective accountability.
   7.2. Custodians are responsible for reviewing and updating component inventories in accordance with property management guidelines.

8. *Software Usage Restrictions [CM-10]*
   8.1. The information owners and custodians are responsible for utilizing licensed software, including open-source software, in accordance with contract terms and copyright laws.
   8.2. The IT division is responsible for tracking the use of software and associated documentation protected by quantity licenses to control copying and distribution.
   8.3. Custodians are responsible for controlling the use of peer-to-peer file-share technologies in accordance with Federal and State regulations and Executive Orders.

9. *User-Installed Software [CM-11]*
   9.1. Users may not install software on information systems that house or process confidential information without the prior consent of the IT Division.
   9.2. Custodians must enforce software installation policy through centrally managed technologies such as SCCM, Intune, MDM, university-approved app stores, etc.
   9.3. Custodians must monitor policy compliance at least every five years.

I. PHYSICAL AND ENVIRONMENTAL PROTECTION.

[Covered in Physical and Environmental Protection Policy].

J. CONTINGENCY PLANNING.

1. *Contingency Plan [CP-2]*
   1.1. The focus of contingency planning in this section of the policy is on the information system. Contingency planning for mission-critical information systems is an important component of the university's Continuity of Operations Planning (CooP). This section does not aim to recreate the CooP, managed by the risk management office. However, custodians can develop contingency planning as part of the CooP that is in compliance with Section 412.054, Labor Code that addresses information resources so that the effects of a disaster will be minimized, and the state agency will be able either to maintain or quickly resume mission-critical functions. At a minimum, the custodian must:
      1.1.1. Develop a contingency plan for the information system in compliance with that:
         1.1.1.1. Identifies essential missions and business functions and associated contingency requirements.
         1.1.1.2. Provides recovery objectives, restoration priorities, and metrics.
         1.1.1.3. Addresses contingency roles, responsibilities, and assigned

individuals with contact information.

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

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

1.1.1.6. Is reviewed and approved by the information owner.

1.1.2. Distribute copies of the contingency plan to the information owner, IRM, personnel responsible for following the contingency plan, and applicable vendors and service providers.

1.1.3. Coordinate contingency planning activities with incident handling activities.

1.1.4. Review the contingency plan for the information system at least every two years.

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

1.1.6. Communicate contingency plan changes to the information owner, IRM, personnel responsible for following the contingency plan, and applicable vendors and service providers.

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

2. *Contingency Training [CP-3]*

2.1. Custodians are responsible for providing training to information system users consistent with assigned roles and responsibilities within 90 days of assuming a contingency role and subsequently when information systems change or at least biennially. For example, users may need to be trained on using a remote access service (VPN) to access information systems during a disaster recovery situation when the information system is running at an alternate site. Technical staff may need to be trained on disaster recovery procedures for the information system. Custodians are encouraged to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

3. *Contingency Plan Testing [CP-4]*

3.1. Custodians are responsible for:

3.1.1. Testing the contingency plan for information systems at least annually, to determine its effectiveness and coordinating with organizational elements such as users and business offices, responsible for related plans.

3.1.2. Reviewing contingency plan test results.

3.1.3. Initiating corrective actions, if needed.

3.1.4. Testing the contingency plan at applicable alternative processing sites.

4. *Alternate Storage Site [CP-6]*

4.1. Custodians must:

4.1.1. Establish an alternate storage site consistent with recovery time objectives (RTO), including necessary agreements to permit the storage and retrieval of information system backup information. Alternate storage sites are sites that are geographically distinct from campus. The purpose of alternative storage sites is to prevent data loss from threats such as natural disasters, structural failures, hostile cyber-attacks, and errors of omission /commission.

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

4.1.3. At a minimum Mission-critical information must be backed up on a scheduled basis and stored off-site in a secure, environmentally safe, locked facility accessible only to authorized state agency representatives.

5. *Telecommunications Services [CP-8]*
   5.1. Custodians are responsible for establishing alternate telecommunications services, including necessary agreements to permit the resumption of essential missions and business functions within applicable RTO when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. Telecommunication services include data and voice services from service providers.

6. *Information System Backup [CP-9]*
   6.1. Custodians are responsible for the following:
      6.1.1. Conduct backups of user-level information contained in the information system consistent with RTO.
      6.1.2. Conduct backups of system-level information contained in the information system consistent with RTO.
      6.1.3. Conduct backups of information system documentation, including security-related documentation consistent with RTO.
      6.1.4. Protect the confidentiality, integrity, and availability of backup information at storage locations by utilizing cryptographic mechanisms as listed in the LTCI [MP-4].
      6.1.5. Test backup information for reliability at least annually and use sample backups in the restoration of selected information functions as part of contingency testing.
      6.1.6. Transfer information system backup to an alternative storage site.

7. *Information System Recovery and Reconstitution [CP-10]*
   7.1. Custodians are responsible for providing tools and technologies for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Examples of tools and technologies can be transactional recovery for systems that are transactional-based and restoration from backups.

8. *Alternate Communications Protocols [CP-11]*
   8.1. *Custodians must have the capability to employ institution-defined alternative communications protocols in support of maintaining continuity of operations.*

V. EXCEPTIONS

A. The ISO, with the approval of the Lamar University President, may issue documented exceptions to controls in this policy based on justifications communicated as part of the risk assessment process.

VI. ENFORCEMENT

A. Failure to adhere to the provisions of this policy statement may result in:
   1. Loss of Lamar University Information Resources access privileges.
   2. Disciplinary action up to and including termination for employees, contractors, or consultants.
   3. Dismissal for interns and volunteers.
   4. Suspension or expulsion in the case of a student.
   5. Civil or criminal prosecution.

VII. RELATED DOCUMENTS

A. Information Technology Policies and Standards Definition Catalog.
B. Texas Business and Commerce Code
C. Texas Administrative Code TAC 202
D. Lamar University Records Retention Schedule

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: IRM

Review Schedule: Every three years

Last Review Date: 11/07/2023

Next Review Date: 11/07/2026

IX. APPROVAL

Jaime Taylor - 01/10/2024
_____
President, Lamar University

Patrick Stewart - 01/10/2024
_____
IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	11/7/2023	**Purpose** **a. TCSC updated to v2.1.** **b. Cloud Services added.** **IA Family** **a. IA[2] – Revised policy statement.** **b. IA[1.3] – "IMDSS" renamed to IT Division.** **c. IA[2(1)] – New policy statement.** **d. IA[2(2)] – New policy statement.** **e. IA[5.1.1] – "Services" added to policy statement.** **a. IA[3.1.6] – Removed from previous policy.** **f. IA[5.2] – New policy statement.** **g. IA[6.2] – Revised policy statement.** **h. IA[5(1) – New policy statement.** **i. IA[6] – New policy statement.** **j. IA[7] – New policy statement.** **b. IA[10] – Removed from previous policy.** **k. IA[11] – New policy statement.** **AC Family** **a. AC[1.1] – "Information Resource Manager (IRM)" added to policy statement.** **b. AC[1.1.2] – New policy statement.** **c. AC[1.1.1.4] – New policy statement.** **d. AC[1.1.4] – Removed from previous policy.** **e. AC[1.2.4] – New policy statement.** **f. AC[1.2.11] – New policy statement.** **g. AC[1.2.12] – New policy statement.** **h. AC[2(3)] - New policy statement.** **i. AC[3] – New policy statement.** **j. AC[2.1.1] – Removed from previous policy.** **k. AC[2.1.2] – Removed from previous policy.** **l. AC[4.1.1] – New policy statement.**

Revision Number	Approved Date	Description of Changes
1	11/7/2023	**AU Family** **a. AU[2] – Revised policy statement.** **b. AU[3] – New policy statement.** **c. AU[5] – New policy statement.** **d. AU[6] – Revised policy statement.** **e. AU[8] – New policy statement.** **f. AU[9] – New policy statement.** **g. AU[11] – Revised policy statement.** **h. AU[12] - New policy statement.** **MA Family** **a. MA[3.1] – "Approve" added to policy statement.** **b. MA[3.2] - Revised policy statement.** **SI Family** **a. SI[1.2] – Removed from previous policy.** **b. SI[2.2] – New policy statement.** **c. SI[3.3] – Revised policy statement.** **d. SI[3.4] – New policy statement.** **e. SI[3.5] – Removed from previous policy.** **f. SI[3.6] – New policy statement.** **g. SI[10] - New policy statement.** **MP Family** **a. MP[4.2] – Removed from previous policy.** **b. MP[4.3] – New policy statement.** **c. MP[4.4] – New policy statement.** **d. MP[5.2.3] – Removed from previous policy.** **e. MP[5.3] – New policy statement.**

Revision Number	Approved Date	Description of Changes
1	11/7/2023	**SC Family** **a. SC[8] – New policy statement.** **b. SC[10] – New policy statement.** **c. SC[13] – New policy statement.** **d. SC[15] – New policy statement.** **e. SC[18] – Removed from previous policy.** **f. SC[19] – Removed from previous policy.** **g. SC[20] – New policy statement.** **h. SC[21] - New policy statement.** **i. SC[22] – New policy statement.** **j. SC[24] – New policy statement.** **k. SC[13.2] - New policy statement.** **l. SC[39] – New policy statement.** **m. SC[43] - Removed from previous policy.** **CM Family** **a. CM[1.6] – New policy statement.** **b. CM[3] - Revised policy statement.** **c. CM[4] – New policy statement.** **d. CM[5] – New policy statement.** **e. CM[9] - Removed from previous policy.** **f. CM[8.2] - "IMDSS" renamed to IT Division.** **g. CM[8.1] – Removed from previous policy** **h. CM[9.1] – New policy statement.** **CP Family** **a. CP[1] – Revised policy statement.** **b. CP[4.1.3] – New policy statement.** **c. CP[7] – Removed from previous policy.** **d. CP[11] – New policy statement.**