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 configuration and management of said systems.

This policy document and the associated Lamar University Technical Control Index incorporate mandated minimum controls from the Texas Control Standards Catalog (TCSC) v1.3 and Texas Administrative Code (TAC) §202.76.a and §202.76.b applicable to information systems management, including servers, networks, 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 Information Owners and custodians. The Lamar University Technical Control Index groups the associated tactical controls. The same tactical control is written in multiple applicable areas: applications, network, 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 and increase consistency of operation and ensure compliance.

Unless specified otherwise, 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 a 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. Information Owners are responsible for identifying Personally Identifiable Information (PII), defined under Texas Business and Commerce Code as information required to uniquely identify users and establish unique electronic identifiers.
   1.2. The Information Management and Decision Support Services (IMDSS) division is responsible for the generation and distribution of centrally managed, unique electronic identifiers for organizational users, for example, LEA username. While it is feasible to generate identifiers, departments are required to utilize the identifiers centrally issued by IMDSS in their information systems to ensure simplicity for users, consistency of authentication, and easier identification in audit processes.
   1.3. Based on the security categorization, the information system must be configured to authenticate users or processes acting on behalf of users, utilizing one or more forms of authentication.

2. *Device Identification and Authentication [IA-3*]
   2.1. 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.

3. *Identifier Management [IA-4]*
   3.1. Custodians that manage identifiers, for example, Usernames, MAC Addresses, IP Addresses, and Device Tokens, must:
      3.1.1. Receive authorization from the Information owner to assign an identifier.
      3.1.2. Develop, document, and maintain a naming convention for identifiers that identify an individual, group, role, or device.
      3.1.3. Select an identifier that identifies an individual, group, role, or device.
      3.1.4. Assign the identifier to the intended individual, group, role, or device.
      3.1.5. Prevent reuse of identifiers.
      3.1.6. Disable the identifier immediately after the individual is no longer affiliated with the university or after 90 days of inactivity.

4. *Authenticator Management [IA-5]*
   4.1. Custodians, during initial authenticator setup, for example, Passwords, Passphrases, and Tokens, must:
      4.1.1. 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.
      4.1.2. Ensure that the authenticator generated complies with the complexity requirements specified in the Security Passwords Standard.
   4.2. Custodians must establish and implement administrative procedures for:
      4.2.1. Initial authenticator distribution, for example, secure email, pre-expired passwords, one-time passwords, dynamic password change links.
      4.2.2. Handling lost/compromised/damaged authenticators.
      4.2.3. Revoking authenticators, for example, disabling accounts.
      4.2.4. Changing authenticators for group/role accounts when membership of those accounts' changes.
      4.2.5. Educating users on specific actions to safeguard authenticators, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately.
   4.3. Custodians must configure information systems to enforce:

4.3.1. The change of default authenticator content during system installation.
4.3.2. The level of authenticator complexity so that it complies with the Security Passwords Standard.
4.3.3. 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.

5. *Identification and Authentication (Non-Organizational Users) [IA-8]*
   5.1. The information system must uniquely identify and authenticate non-organizational users or processes acting on behalf of a non-organizational user.
   5.2. In most circumstances, the identification requirements for a non-organizational user must be treated similarly to an organizational user. An electronic identity 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.
   5.3. The Information Owner, in consultation with the Office of the Information Security Officer (ISO), can authorize the use of an external identity 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] as specified in the Lamar University Technical Control Index.

6. *Adaptive Identification and Authentication [IA-10]*
   6.1. Custodians that access very high privileged accounts must require additional factors of authentication as specified by the Office of the ISO.

B. ACCESS CONTROL

1. *Account Management [AC-2]*
   1.1. For each information system, the Information Owner, working in conjunction with the custodian and the Office of the ISO, either through manual or automated mechanisms, must:
      1.1.1. Assume the role of the account manager.
      1.1.2. Specify authorized users of an information system, group and role membership, access authorization, and other attributes for each account.
      1.1.3. Authorize access to information systems based on:
         1.1.3.1. Intended system usage.
         1.1.3.2. 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.
      1.1.4. Review accounts for the privileges assigned, validate the need for such privileges, at least annually, and re-assign or remove privileges, as necessary.
      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. Require approval from the Information Owner to create information system accounts.

1.2.5. Create, enable, modify, disable and remove information system accounts in accordance with Information Owner defined conditions, such as valid access authorization.

1.2.6. Notify the Office of the ISO and the Information Resource Manager (IRM) of the creation, modification, enabling, disabling, and removal actions for very high privileged accounts.

1.2.7. 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.

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

1.2.9. Notify the Information Owner when:

1.2.9.1. Accounts are no longer required.

1.2.9.2. Users are terminated or transferred.

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

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

1.2.11. 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.

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

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

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

2. *Separation of Duties [AC5]*

2.1. Separation of duties addresses the potential of abuse of authorized privileges and assists in reducing the risk of malevolent activities. The Information Owner is responsible for:

2.1.1. Separating the duties of individuals based on responsibilities.

2.1.2. Documenting the separation of duties.

2.1.3. Defining information system access authorization to support the separation of duties.

3. *Least Privilege [AC-6]*

3.1. The principle of least privilege ensures that users and processes acting on behalf of users operate at privilege levels no higher than necessary to accomplish mission or business functions. Information Owners must incorporate the principle prior to authorizing access.

3.2. Information Owners must establish processes and procedures to explicitly authorize access to security functions, which includes any network-based privilege access.

3.3. 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,

3.4. Custodians must select and enforce the least privileged roles when enforcing access control within the information system.

3.5. 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).

3.6. 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.

4. *Permitted Actions without Identification or Authentication [AC-14]*
   4.1. When the information system or portions of the information system functionality permits user actions without the need for identification or authentication, such functionality and its rationale must be documented in the Security Plan for the information system.
   4.2. 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.

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

6. *Wireless Access [AC-18]*
   6.1. Wireless networks must be configured based on the connection requirements provided in the Lamar University Technical Control Index.
   6.2. Custodians must disable 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.

7. *Access Control for Mobile Devices [AC-19]*
   7.1. 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.

8. *Use of External information systems [AC-20]*
   8.1. 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:
      8.1.1. Access the information system from external information systems.
      8.1.2. Process, store, or transmit institution-controlled information using external information systems.

9. *Information Sharing [AC-21]*
   9.1. Authorized users may share confidential, sensitive, regulated information with contracted sharing partners only with the explicit permission of the Information Owner.

10. *Publicly Accessible Content [AC-22]*
    10.1. 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 and remove such information if discovered and notify the Office of the ISO.

C. AUDIT AND ACCOUNTABILITY

1. *Audit Events [AU-2]*
   - *1.1.* At the point of acquisition, information systems must be evaluated to ensure that they are capable of auditing the events listed in the auditable events and log content standard.
   - *1.2.* The Office of the ISO is responsible for the coordination of the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

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

3. *Audit Review, Analysis, and Reporting [AU-6]*
   - 3.1. Custodians are responsible for monitoring and reviewing audit logs to identify and report inappropriate or unusual activity to the Office of the ISO.

4. *Audit Record Retention [AU-11]*
   - 4.1. Archived audit records that are no longer needed for administrative, legal, audit, or other operational purposes must be retained for a minimum of 90 days.

5. *Cross-Organizational Auditing [AU-16]*
   - 5.1. 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 and repairs on information system components in accordance with manufacturer or vendor specifications.
     - 1.1.2. Approve and monitor all maintenance activities, whether performed on-site or remotely, and whether the equipment is serviced on-site or removed to another location.
     - 1.1.3. Seek explicit approval from the Information Owner prior to the removal of information systems that process SPI or Confidential information from the organizational facilities for off-site maintenance or repairs.
     - 1.1.4. Remove all data from associated media, using an approved non-recoverable technique prior to removal for off-site maintenance or repairs, 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 or repair actions.
     - 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 and monitor any nonlocal maintenance and diagnostic activity. This includes any remote sessions with contracted vendors or service providers.

3.2. The Office of the ISO must be notified of diagnostic tools that alter the security posture of the information system, for example, such tools that exhibit the following characteristics:

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, 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 refers 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. Custodians are responsible for remediating vulnerabilities and flaws within 30 calendar days of identification or notification. 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.

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

1.4. Custodians must install security-relevant software and firmware updates within 30 calendar days of the release of the update.

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

2. *Malicious Code Protection [SI-3]*

2.1. Custodians must employ centrally managed and automatically updated malicious code protection mechanisms on information systems 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 the malicious code protection mechanism to:

2.2.1. Perform weekly, full scans of the information system and real-time scans of files.

2.2.2. Audit the detection of any malicious code.

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

2.3. 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 deploy software or hardware monitoring devices that are approved by the Office of the ISO to collect the information specified in the auditable events and log content standards.

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

3.5. Custodians must increase the level of information system monitoring activities in response to indications of credible increased risk.

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

3.7. Custodians must provide the information specified in auditable events and log content standards, 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, etc., on an on-going 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 Handling and Retention [SI-12]*

6.1. 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, university data retention standards, and guidelines.

F. MEDIA PROTECTION

1. *Media Access [MP-2]*

1.1. Information system media include both digital and non-digital media. Access to information system media that contains confidential or regulated information must be restricted to organizational user or role.

2. *Media Marking [MP-3]*

2.1. Custodians must mark portable information system media indicating the highest classification of data stored on the media.

Non-portable media types, for example, relational databases, are exempted from marking as long as the media on which they reside remains within the university's information processing facilities.

3. *Media Storage [MP-4]*

3.1. All information system users are responsible to securely store digital and non-digital media within physically controlled areas. Examples of physical control include a locked drawer, desk, cabinet, or controlled media library.

3.2. Digital media containing confidential or regulated information must implement cryptographic mechanisms as specified in the Lamar Technical Control Index to protect the confidentiality and integrity of the information.

4. *Media Transport [MP-5]*

4.1. Non-digital media containing confidential or regulated information that leaves controlled areas must be protected by physical safeguards, such as locked storage, during transport.

4.2. Digital media containing confidential or regulated information that leaves controlled areas must implement cryptographic mechanisms as specified in the Lamar Technical Control Index to protect the confidentiality and integrity of stored information.

4.3. For information system media that contain confidential or regulated information, Custodians must:

4.3.1. Maintain accountability for the information system media during transport.

4.3.2. Document activities associated with the transport of information system media.

4.3.3. Restrict the activities associated with the transport of information system media to authorized personnel.

5. Media Sanitization [MP-6]

5.1. Custodians are responsible for maintaining the documentation of equipment disposition. Media containing confidential information must be disposed of according to the following criteria.

5.1.1. Non-digital media that contain confidential or regulated information must be

physically destroyed by shredding prior to leaving university premises.

5.1.2. 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.

5.1.3. Equipment with non-removal digital media, such as network devices, must be factory reset prior to sending them back for repairs to ensure university configurations are erased.

5.1.4. 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.

5.2. Custodians must follow additional steps for equipment that are under warranty, lease, or contract.

5.2.1. If equipment has non removeable media, is under warranty and needs to be sent back for repair/RMA, custodians must factory reset before sending the equipment.

5.2.2. Custodians must obtain a certificate of data destruction from vendors when equipment is returned at lease end.

5.2.3. Portable digital media such as CD-ROMs, USB Flash drives, Memory cards, etc., must be physically destroyed when the media has reached the end of useful life.

5.2.4. When financially feasible, custodians must 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. Any removed digital media must be physically destroyed such that data cannot be reconstituted.

5.2.5. If removal of digital media violates the terms of warranty, then the custodians must cryptographically erase the digital media prior to return of equipment to the manufacturer, RMA or repair.

6. *Media Use [MP-7]*

6.1. 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.

6.2. 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.

7. *Media Downgrading [MP-8]*

7.1. 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.

7.2. 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 utilization and capacity of the information system when managing risk from Denial of Service (DOS) due to malicious attack.

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 malicious attack, to the Office of the ISO.

2. *Boundary Protection [SC-7]*

2.1. Custodians must work, in conjunction with the Office of the ISO, to monitor and control communications at the external boundary of the information system by:

2.1.1. Implementing a managed interface for each external telecommunication service.

2.1.2. Establishing a traffic flow policy for each managed interface.

2.1.3. Protecting the confidentiality and integrity of the information being transmitted across each interface.

2.1.4. Documenting exceptions to the traffic flow policies in the information system security plan.

2.1.5. Reviewing exceptions to the traffic flow policy when substantial changes are made and remove exceptions that are no longer required.

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. Custodians must implement boundary protection mechanisms to segment information systems that house or process confidential or regulated information.

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

3.1. 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.

3.2. 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.

4. *Public Key Infrastructure Certificates [SC-17]*

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

4.2. 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.

4.3. 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.

5. *Mobile Code [SC-18]*

5.1. Custodians must obtain authorization from the Office of the ISO prior to the procurement or deployment of applications that house or process confidential information that are built on mobile code technologies such as Java, JavaScript, etc.

6. *Voice Over Internet Protocol [SC-19]*

6.1. Custodians must segment networks used for university business communications that utilize Voice Over Internet Protocol (VOIP) technologies such as the university's phone systems to prevent eavesdropping and malicious use.

7. *Protection of Information at Rest [SC-28]*

7.1. Custodians must protect the confidentiality and integrity of confidential and regulated

information at rest utilizing encryption standards specified in the Lamar University Technical Control Index.

8. Usage Restrictions [SC-43]

8.1. Custodians are responsible for physically securing information system components such as photocopiers, scanners, printers, optical devices, barcode readers, credit card readers, etc., both when in use and not in use.

H. CONFIGURATION MANAGEMENT

1. Baseline Configuration [CM-02]

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.

2. Configuration Change Control [CM-03]

2.1. Changes to the configuration of information systems that house, or process confidential or regulated information must be controlled. Controlled changes are generally known as “Change Control” or “Change Management.” The dedicated Change Management policy covers the following:

2.1.1. Types of changes to the information systems.

2.1.2. Proposed change, approval, or disapproval of such changes.

2.1.3. Security impact analysis.

2.1.4. Processing and procedures that document, implement, and audit changes to the information system.

2.1.5. Organizational entities that coordinate, communicate, and provide oversight for change control activities.

2.1.6. Access restrictions and records of maintenance that support after-the-fact actions to discover unauthorized changes. Security Impact Analysis [CM-04]

2.2. The Office of the ISO must analyze changes to the information system to determine potential security impacts at the installation (prior to “go-live”) and as part of the Change

Management process during the operational lifecycle of the information system.

3. *Configuration Settings [CM-06]*
   3.1. Custodians must:
      3.1.1. 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.
      3.1.2. Implement the configuration settings.
      3.1.3. Identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements.
      3.1.4. Monitor and control changes to the configuration settings in accordance with university policies and procedures.
4. *Least Functionality [CM-07]*
   4.1. During configuration of the information system, custodians must utilize the principles outlined in the Lamar University Technical Control Index to provide only essential capabilities.
   4.2. Insecure ports and services that are documented in the Lamar University Technical Control Index are prohibited from use in production environments.

5. *Information System Component Inventory [CM-08]*
   5.1. Custodians are responsible for developing, documenting, and maintaining, as part of the baseline, an inventory of information system components that:
      5.1.1. Accurately reflects the current information system.
      5.1.2. Includes all components of the information system within its Authorization Boundary.
      5.1.3. Includes a level of granularity necessary for reporting, tracking, and achieving effective accountability.
   5.2. Custodians are responsible for reviewing and updating component inventories in accordance with property management guidelines.

6. *Configuration Management Plan [CM-09]*
   6.1. The Division of IMDSS is responsible for the planning, documentation, and implementation of configuration management.

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

8. *User Installed Software [CM-11]*
   8.1. [Covered in the Acceptable User Policy (AUP)].
   8.2. Custodians must enforce software installation policy through centrally managed technologies such as SCCM, Intune, MDM, the University approved app stores, etc.
   8.3. 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 CooP. At a minimum, the custodian must:

1.1.1. Develop a contingency plan for the information system 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 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 every two years 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.

5. *Alternate Processing Site [CP-7]*

5.1. Custodians must:

5.1.1. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of information systems required for mission-critical business functions within RTO when the primary processing capabilities are unavailable. For the purpose of this policy, alternate processing sites are sites that are geographically distinct from campus. Alternative processing sites help prevent data loss from threats such as natural disasters, structural failures, hostile cyber-attacks, and errors of omission /commission. Campus-based secondary processing facilities may be adequate to mitigate a subset of threats listed above.

5.1.2. Ensure that equipment and supplies required to transfer, and resume operations are available at the alternate processing site, or contracts are in place to support delivery to the site within the defined time period for transfer/resumption.

5.1.3. Ensure that the alternate processing site provides information security safeguards equivalent to those of the primary site.

6. *Telecommunications Services [CP-8]*

6.1. 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.

7. *Information System Backup [CP-9]*

7.1. Custodians are responsible for the following:

7.1.1. Conduct backups of user-level information contained in the information system consistent with RTO.

7.1.2. Conduct backups of system-level information contained in the information system consistent with RTO.

7.1.3. Conduct backups of information system documentation, including security-related documentation consistent with RTO.

7.1.4. Protect the confidentiality, integrity, and availability of backup information at storage locations by utilizing cryptographic mechanisms as listed in the Lamar University Technical Control Index [MP-4].

7.1.5. Test backup information for reliability at least annually and use sample backups in the restoration of selected information functions as part of contingency testing.

7.1.6. Transfer information system backup to an alternative storage site.

8. *Information System Recovery and Reconstitution [CP-10]*

8.1. 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.

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

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: N/A

Next Review Date: 05/14/2024

IX. APPROVAL

_____
President, Lamar University

_____
IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes