LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

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

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

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/compromis/TT2 (y)]Ty-1.15 Td (r)-1.30.001 Tww6.1 (ut(,)3 (

0

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

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

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 a

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 t1 Two92Tj1.3 (i6 0 Td ( )0.f)-4

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.

eve6.1 ( )0ae1.7 (at)3.6 (i)1 (at)3.6 (ed)]TJ,4 (6)3 (nt)3.6 (a s( )Tj5.001 2 ea8

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.

Ngd[(.2 (i)2 (f)l3 (m)7.77o20 Tw 3.4.15 Td()2)Tj0.001 Tc -0.001 Tw30.9641 Tc -0.0N fystem. .

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, [illegible]

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

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 w m (i)1.4 nig0sTc 0on

aCJTs195 (ni)7.5udri i lE272 Tw [(nf)3.6164[(C)-710.005 Tc[-1.3 ( )]TJ0n0.033 T a

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

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 ,ra w (ov)-85 (f)0.56 ( )0.5 (t)0.6(r)-2.(

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

1.5.

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-

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. e[.5 (mC.6 (h)6P.701 0 Td( )Tjr-27erTc 0.2-4 Tw 0.263 0 66.161 TdT

5. *Telecommunications Services [CP-8]*

5.1.

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**	**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] –**