LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technology
AREA: End User Area Number: 10.01.08

SUBJECT: Appropriate Use Policy

I. PURPOSE

Information resources are vital assets used to support the education, research, and administrative activities of Lamar University in pursuit of its mission.

The purpose of this policy is to provide rules that govern the appropriate use and management of Lamar University's information resources by all users and educate them on the responsibilities that they assume when using these resources, as well as to achieve compliance with applicable statutes, regulations, and mandates.

This policy does not reiterate information resource use covered by other university policies hence it is the responsibility of each user to read all information technology and other university policies for a comprehensive understanding of appropriate use of information resources.

Also applicable are university policies prohibiting harassment, plagiarism, and unethical conduct. Laws that apply to the use of Lamar University's information resources include laws pertaining to theft, copyright infringement, insertion of malicious software.

II. SCOPE

This policy applies to all users of Lamar University information resources (e.g., employees, faculty, students, alumni, agents, consultants, contractors, volunteers, vendors, temps, etc.), including custodians and users who have been granted access and privileged access, whether administered remotely, centrally or departmentally, and regardless of where they reside.

Information resources and access are provided for accomplishing tasks related to Lamar University's mission statement.

Censorship is not compatible with the goals of Lamar University. The university will not limit access to any information due to its content, as long as it meets the standard of legality and otherwise complies with Lamar University policy. The university may restrict the use of or access to its information resources to specific research, teaching, or other purposes in keeping with the mission.

However, the university reserves the right to impose reasonable time, place, and manner restrictions on expressive activities or to deny access to use its information resources. The university does not consider computer information resources as a public forum. Furthermore, the university reserves the right to block or impose necessary safeguards against malicious software, websites, and phishing emails, that inherently pose a threat to the confidentially, integrity, or availability of information resources for the university and its stakeholders.

III. DEFINITIONS

See Definition Catalog Version 4 or higher.

IV. ROLES AND RESPONSIBILITIES

A. IDENTIFICATION AND AUTHENTICATION

Account credentials (usernames and passwords) are mechanisms by which users gain access to the multitude of Lamar University information resources. Protection of credentials by the user forms the foundation to protect the confidentiality of information stored within the information resource. The following sections describe credential responsibilities and security.

1. *Lamar ID/LNumber/Username, [Identifiers]*
   1.1. Lamar University users are responsible for:
      1.1.1. All activities that occur within the information system under their identifiers and are subject to local, state, and federal laws governing interactions that occur on university information resources.
      1.1.2. Safeguarding identifiers assigned by Lamar University.
      1.1.3. Not disclosing or sharing identifiers with other individuals, except to university employees.
      1.1.4. Using any non-unique identifiers only for the purposes intended. For example, shared and department accounts and mailboxes must not be used to log into endpoints for regular operations.
      1.1.5. Notifying the office of the ISO of account credentials posing a significant risk to the organization upon the discovery of the risk. For example, if LEA account credentials are discovered posted on the internet.
   1.2. Lamar University users are not permitted to:
      1.2.1. Use identifiers assigned to other users.
      1.2.2. Abuse privileges granted to them to tamper with identifiers without authorization. For example, change a username.
      1.2.3. Generate additional identifiers without authorization. For example, using an administrator account to elevate or generate standard accounts.
      1.2.4. Use non-unique identifiers (such as generic usernames or shared usernames) unless risk analysis has been performed that demonstrates the lack of need for individual accountability, and the exception is approved by the office of the ISO.

2. *Password/PIN/Hardware Tokens [Authenticators]*
   2.1. Lamar University users must:
      2.1.1. Change authenticators from default assignment on first use.
      2.1.2. Change authenticators when lost, stolen, or suspected to be compromised.
      2.1.3. Report lost, stolen, or suspected compromised authenticators to the office of the ISO.
      2.1.4. Safeguard digital and physical authenticators.
      2.1.5. Keep personal devices used as additional factors of authentication (MFA apps), such as phones updated to manufacturer supported OS and locked when not in use.
      2.1.6. Report the discovery of publicly accessible authenticators, such as on monitors, under keyboards or laptops to the office of the ISO.
      2.1.7. Refrain from re-using authenticators used to access Lamar University information resources on external information systems not associated with the university.
      2.1.8. Follow Lamar University standards when generating and using authenticators, such as passwords.

2.1.9. Return any physical authenticators, such as hardware tokens, issued by the university either when no longer required or upon termination of employment or affiliation with the university.

2.2. Lamar University users must not:

2.2.1. Disclose or share authenticators with other individuals, including university employees.

2.2.2. Solicit authenticators from other users.

2.2.3. Post authenticators in publicly accessible areas such as on monitors, under keyboards, or laptops.

2.2.4. Store or transmit authenticators in clear text in communication channels such as emails, instant messenger, or text messages.

3. *Lamar University managed devices:*

3.1. Lamar University users are not permitted to:

3.1.1. Tamper with information that is used to uniquely identify and authenticate organizational managed information systems. For example, Mac Addresses, IP Addresses, device certificates, license keys, unique identifiers, etc.

3.2. Lamar University users that:

3.2.1. Utilize university managed endpoint devices, which require registration with external service providers, such as Apple ID, Google etc. must utilize their university issued identifiers or university issued email addresses.

B. ACCESS CONTROL

Authorized users of Lamar University may have varying degrees of access to both internal and external information resources that store and process confidential and regulated information. Additionally, certain users may be granted privileged access to manage information systems. This section describes the responsibilities and use of access controls and privileges when accessing information systems.

1. *Use of Information Resources*

1.1. Occasional personal use of university information resources is tolerated. Any such use is subject to review and restriction by management. Information resources may not be used in an extensive recurring manner for activities that are unrelated to Lamar university educational purposes. Such personal use must not:

1.1.1. Violate any applicable policies or statutes.

1.1.2. Interfere with the users' job performance.

1.1.3. Result in any additional expense to Lamar University.

1.1.4. Be used for personal gain or personal profit.

1.2. Custodians may monitor the usage of information system accounts for patterns of atypical usage.

1.3. Users must only use information resources for which they are authorized.

1.4. Users may not have any expectations to gain or retain access to university information resources after all affiliation with the university is terminated. For example, access to LEA or Email may be revoked upon termination of employment, unless the user has a continued affiliation with the university.

1.5. To protect university information resources, the university may:

1.5.1. Query the presence of malicious code protection mechanisms on unmanaged devices such as personally owned devices prior to permitting access to information resources and may refuse access if device is not deemed to be adequately protected.

1.5.2. Block malicious code on personally owned systems and storage devices attached to information systems.

1.5.3. Block computationally intensive technologies such as cryptocurrency mining that slows performance for legitimate users, leaves openings for malicious activities, increases electricity and computing costs, ties up technology

staffing resources or increases security and privacy risks.

2. *Privileged Access*
   2.1. Lamar University users must:
      2.1.1. Use privileged accounts only for privileged activities.
      While it may be 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 users' knowledge or intervention.
      2.1.2. Default to unprivileged accounts when using information systems, particularly when accessing untrusted networks such as the Internet.
      2.1.3. Not use privileged accounts to grant privileges to unprivileged accounts, unless authorized by the IRM or the ISO.
   2.2. Lamar University users are not permitted to:
      2.2.1. Tamper or circumvent access control restrictions, naming conventions, information system settings that prevent unauthorized access and management tools enforced by information owners or custodians.

C. AUDIT AND ACCOUNTABILITY

Information system audit logs are used to establish accountability. Audit logs also help track changes made within information systems and diagnose potential problems. Maintaining the integrity of audit settings and logs is critical. The following section describes the rules governing audit logs.

1. *Audit Logs*
   1.1. Lamar University users:
      1.1.1. Should not have any expectation of rights to privacy of information contained in audit events. Audit events captured by information systems may be used by the university for the purposes of incident response, service delivery, automation and optimization and can sometimes contain portions of Personally Identifiable Information (PII) or can be correlated to PII such as names, timestamps, network addresses, unique identifiers.

   1.2. Lamar University users are not permitted to:
      1.2.1. Tamper with or circumvent audit settings enforced by custodians, in the information system.
      1.2.2. Tamper with technologies used to protect the integrity of audit events generated by information systems.
      1.2.3. Tamper with technologies used to ensure non-repudiation.
      1.2.4. Alter or delete audit events generated by information systems.

D. MAINTENANCE

Maintenance is necessary to preserve the security and integrity of information systems and to avoid security incidents and breaches. Proper maintenance ensures that systems are consistently kept up to date. Maintenance requires privileged access and is therefore important that it is performed by authorized university personnel utilizing approved management tools.

1. *Controlled Maintenance*
   1.1. Lamar University users:
      1.1.1. Are required to contact authorized university personnel to request assistance for hardware and software maintenance.
      1.1.2. Must explicitly terminate remote maintenance sessions and associated network connections when remote maintenance is completed.

1.1.3. When participating in remote maintenance sessions, not leave the information system unattended.

1.2. Lamar University users are not permitted to:

1.2.1. Perform software maintenance, audits, or configuration on information systems. In this context, software maintenance refers to operating systems, installations, upgrades, and replacement.

1.2.2. Install maintenance tools on information systems without explicit approval from custodians.

1.2.3. Allow third-party entities not specifically contracted by Lamar University to perform maintenance on any information system owned by the University. Examples of third-party entities include Best Buy technical support and callers that claim to be affiliated with companies such as Microsoft.

1.2.4. Utilize remote maintenance tools that alter the security posture of the information systems. For example, maintenance tools that exhibit the following characteristics: back door with persistent presence, copy or exfiltrate data, hardcoded credentials, auto-discovery of devices or services, periodic contact to or from external sites, persistent debug mode that captures confidential or sensitive information in logs.

1.2.5. Participate in remote maintenance sessions such as screen shares that do not utilize strong authenticators, one-time passwords, or one-time use sessions.

E. SYSTEM AND INFORMATION INTEGRITY

Maintaining a strong information security posture requires preventing unauthorized access, protecting information systems from malicious code such as viruses and worms, and addressing known vulnerabilities in a timely manner. The following section establishes certain rules regarding the operations of these protection mechanisms.

1. Information System Protection

1.1. Lamar University users are required to:

1.1.1. Follow established procedures for safeguarding information system outputs. For example, protect monitor screens from shoulder surfing and safeguard printer outputs.

1.2. Lamar University users are responsible for reporting to custodians:

1.2.1. When they become aware of vulnerabilities in the university's information systems.

1.2.2. Malfunction or security alerts generated by malicious code protection mechanisms. Malicious code mechanisms include software such as antivirus, Endpoint Detection and Responses solutions (EDR).

1.3. Lamar University users are responsible for reporting to the office of the ISO:

1.3.1. Errors with malicious code detection mechanisms. Examples of errors can be legitimate files or programs being identified incorrectly as malicious (false positives).

1.4. Lamar University Users are not permitted to:

1.4.1. Tamper or circumvent malicious code protection mechanisms installed by custodians on university information systems.

1.4.2. Initiate attacks on university information resources or personally owned systems.

1.4.3. Knowingly infect university information systems.

1.4.4. Visit known malicious websites.

1.4.5. Experiment with or deploy tools and techniques that circumvent the security posture of the university's information resources.

1.4.6. Maliciously degrade the performance of information resources.

1.4.7. Deprive an authorized user access to an information resource.

1.4.8. Circumvent configured authentication mechanisms on information systems.

F. MEDIA PROTECTION

The appropriate destruction and disposal of digital and non-digital media is important to avoid the disclosure of university-controlled confidential, regulated, or sensitive information following use.

1. *Media Disposal and Sanitization.*
   - *1.1.* Lamar University users are responsible for the secure disposition of:
     - *1.1.1.* Non-digital media by utilizing designated shredding services. For example, shredding printed documents when no longer required.
     - *1.1.2.* Digital media, such as computers, tablets, iPads, laptops, servers, copiers, portable storage devices, flash drives, by following procedures established by the Property Management office. (IT equipment removal request).

G. SYSTEM AND COMMUNICATION PROTECTION

Modern cloud environments offer several services available over the internet to users (either free or paid) that offer storage and processing. While certain services may be adequate for personal information, the services may not offer adequate protection to ensure the confidentiality of information for the organization. Hence the university contracts with selected service providers that meet the universities standards for security and compliance. Additionally, employees may have access to university-controlled confidential and regulated information that require due diligence and due care for its protection.

1. *Cloud and Personal Storage*
   - 1.1. Lamar university users are not permitted to:
     - 1.1.1. Use unauthorized external or cloud-hosted information resources for the purposes of accomplishing university business, research, or instructional purposes that would involve the collection, storage, processing, or transmission of sensitive or confidential university data. For example, storing FERPA protected course information on personal USB drives, Google Drive, iCloud.

2. *Transmission Confidentiality and Integrity*
   - 2.1. Lamar university employees are responsible for:
     - 2.1.1. Utilizing cryptographic technologies such as encryption with, at minimum, 128bit encryption algorithm when transmitting university-controlled confidential or regulated information over a public network, for example, the Internet. Users must contact the office of the ISO for assistance in determining the appropriate cryptographic technology.
     - 2.1.2. Ensuring that endpoints are locked when leaving them unattended.
     - 2.1.3. Securing cryptographic keys to prevent the loss of data by following the procedures established by the office of the ISO.
     - 2.1.4. Protecting the confidentiality and integrity of confidential and regulated information at rest by utilizing encryption standards as specified by the office of the ISO.

H. CONFIGURATION MANAGEMENT

Software is distributed with licensing terms and conditions of use by the publishers, which outline the conditions of its use. Ensuring that software is kept updated is an important component of maintaining information resources secure.

1. *Software and Endpoints*

1.1. Lamar University users are responsible for:
1.1.1. Understanding and complying with licensing terms for software in accordance with contract terms and copyright laws. For example, not using personally licensed software for business.
1.1.2. Updating software and operating systems on personally owned devices prior to connecting to university network or accessing university services, so that the devices remain compatible with university services and do not pose potential threats to its information resources.
1.2. Lamar university users may not use:
1.2.1. Certain technologies such as peer to peer file-sharing.
1.2.2. Technologies that are restricted by federal and state laws and executive orders. when connected to the university's network.

I. CONTINGENCY PLANNING

Under certain circumstances it may be necessary for Lamar University users to access information resources from locations other than primary campus and offices. This section sets forth rules concerning work locations, communication channels and information resources.

1. *Alternate Work Location*
1.1. Lamar University users are responsible for:
1.1.1. Ensuring the security and privacy of information when working from alternative work locations. For example, employees working from locations such as home or hotel are expected to exercise all precautions to maintain the security and privacy of the information. It is also expected that Lamar University users will take precautions to protect university issued devices against damage, theft, and loss.

2. *Alternative Communications Channel*
2.1. Lamar University may authorize users to:
2.1.1. Utilize alternative communication channels or information resources to ensure continuity of operations in the event of Disaster Recovery (DR), when primary communication channels or information resources become unavailable.

J. SERVICE ACQUISITION

In order to maintain the security of new and acquired information resources, applicable contracts that meet the needs of the university must be agreed upon and services purchased through the appropriate channels and approved by the appropriate personnel. When university-controlled information is required to be supplied to third party service providers, the university still holds the responsibility of ensuring that the information is protected.

1. *Contractual Agreements*
1.1. Lamar University users who:
1.1.1. Individually engage third-party products or services by unauthorized acceptance of Terms of Service or Terms of Use agreements on behalf of the university (online, click-through or otherwise) are personally responsible and liable for any obligations incurred by the agreement, as well as any consequences that may result from their engagement with the third-party.

2. Acquisitions
2.1. Lamar University users are not permitted to:
2.1.1. Purchase information systems peripherals without prior authorization.
2.1.2. Engage third-party products, services, extensions, etc., non-browser plugins

and add-ons, without prior authorization through the service and acquisition process, regardless of the cost of the product or service.

2.1.3. Supply university-controlled confidential, regulated, or sensitive information to third-party entities during the process of evaluation of information resources without a contractual agreement such as a Non-Disclosure Agreement (NDA). Evaluation of information resources generally refers to offers such as free trials, proof of concepts, pilot programs, try before you buy software, applications, or Software as a Service (SaaS) products, etc.

2.1.4. Modify or change the information system or operating system in a manner that voids the manufacturer's warranty.

3. Licensing

3.1. Any software and other information resources acquired or licensed by Lamar University are the property of the university or the company from whom it is licensed. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these may constitute a computer-related crime punishable under state and federal statutes.

K. SECURITY AWARENESS AND TRAINING

Lamar University is mandated by the state to provide security awareness training to employees. The training is intended to provide users with the relevant experience to identify threats such as phishing and social engineering as well as other IT Security guidance to keep users and systems secure while using Lamar University's information resources.

1. Cybersecurity Awareness

1.1. Lamar University Employees must:

1.1.1. Complete all assigned cybersecurity awareness training.

L. MISUSE AND ABUSE OF INFORMATION RESOURCES

The misuse and abuse of Lamar University's information resources can lead to the unavailability of systems, impact security posture and prevent authorized users access to the information resource. Lamar University can address issues and proactively protect affected systems when misuse and abuse are reported.

1. Patterns of Abuse

1.1. Lamar University considers the abuse of information resources as, but not limited to, any willful act that:

1.1.1. Endangers or damages any information resource, regardless of logical or physical location.

1.1.2. Disrupts or degrades the availability of information resources.

1.1.3. Intentionally occupies or monopolizes information resources for an unreasonable period of time to the detriment of other authorized users.

1.1.4. Introduces malicious software or data into information resources intended to affect the information resource's confidentiality, integrity, or availability.

1.1.5. Sends a message with the intent to disrupt university operations or operations of external entities.

1.1.6. Attempts to use, access, duplicate, disclose, alter, damage, or destroy any physical or electronic data repository or other information resources without appropriate authorization.

1.1.7. Attempts to use Lamar University information resources to target other information resources.

1.1.8. Attempts to destroy or alter evidence explicitly preserved due to a litigation hold or preservation request. Generally considered as "Spoilation of

evidence"

2. *Report of Abuse*
   2.1. Lamar University users are responsible for:
      2.1.1. Reporting any abuse or misuse of information resources to the Information Technology Services.

M. NETWORK USAGE

Lamar University's network is a critical component for the university to fulfil its mission. The network provides connectivity between information resources. ~~A~~ stable and reliable network ensures uninterrupted and secure access to information resources.

1. *Wired and Wireless Network*
   1.1. Lamar University users are not permitted to:
      1.1.1. Modify, extend, or disrupt the university's network. For example, adding hubs, switches, wireless access points, add alterations to the physical network, like modifying or extending a wall data port or similar devices.
      1.1.2. Perform unauthorized network scanning, fingerprinting, eavesdropping, or penetration testing or conduct other reconnaissance activities on information resources.
      1.1.3. Perform unauthorized alteration or relay of network traffic. For example, "man-in-the middle" attacks.

N. COPYRIGHT AND INTELLECTUAL PROPERTY

Most software and many digital materials are covered by some form of copyright, trademark, license, or agreement with potential civil or criminal liability and penalties. The copyright or trademark holder must specifically authorize duplication, use or distribution, or a specific exception of the Copyright Act, such as the Fair Use exception, the Library exception, or exceptions under the TEACH Act. Intellectual property laws extend to the electronic environment.

1. *Copyright Infringements*
   1.1. Lamar University users are not permitted to:
      1.1.1. Duplicate, use or distribute software or other copyrighted materials without authorization. For example, Music, Graphics, Videos, etc.

2. *Intellectual Property (IP)*
   2.1. Lamar University users should:
      2.1.1. Assume that works communicated through the university network and any of its information resources are subject to copyright laws, unless specifically stated otherwise.

O. PRIVACY AND RIGHTS.

During the course of normal business operations, Lamar University continuously collects, stores, processes, monitors, shares, and deletes user data. This data may be explicitly provided by the users or implicitly generated when users access university information resources.
Lamar University complies with state and federal law protecting the confidentiality of certain types of information that may be maintained on university information resources. For example, education information, protected health information, and other sensitive personal data and identifiers.

1. *Expectation of privacy*
   1.1. Unless guaranteed by state or federal regulations, while using university information resources, users may not have any expectations of rights to privacy. All user activity may be subject to monitoring, logging, and review.
   1.2. The university cannot guarantee absolute privacy or confidentiality of digital documents or communications when:
      1.2.1. Personal devices are attached to the university's information system. For example, portable storage connected university computers or personal devices connected to the university network.
      1.2.2. Personal data is stored on university information resources.
      1.2.3. Using official communication channels.

2. *Disclosure Expectations.*
   2.1. Although ongoing monitoring is not standard procedure, anyone using Lamar University's information resources consents to being monitored. If such monitoring reveals evidence of possible criminal activity, Lamar University officials may provide that evidence to law enforcement.
   2.2. Information resource usage is subject to review and disclosure in accordance with:
      2.2.1. The Texas Public Information Act, the federal Freedom of Information Act, and other related laws, Regents Rules, and Lamar University policies.
      2.2.2. Other policies or legal requirements, such as subpoenas and court orders.
      2.2.3. Efforts to protect and sustain operational performance and integrity.
      2.2.4. Applicable policies for any purposes that allow Lamar University officials to fulfill their responsibilities when acting in their official capacity.

P. DATA SECURITY AND REPRESENTATION

Data Security is everybody's responsibility. Lamar University takes reasonable precautions, which are industry standards, to protect the data under its control. Reports from users are a key component of protection when data is discovered to be exposed to unauthorized users.

1. *Use of External Information Resources*
   1.1. Lamar University users are not permitted to:
      1.1.1. Process, store, or transmit university-controlled confidential, regulated, or sensitive information, using external information systems, managed by providers that do not have any trust relationships with the university. Trust relationships are contracts between the university and third-party providers, signed by the VP of finance.
      1.1.2. Store university-controlled confidential, regulated, or sensitive information on unsanctioned cloud service providers. For example, Apple iCloud, Google Storage or Dropbox.

2. *Data Exposure*
   2.1. Lamar University users are responsible to report to the office of the ISO:
      2.1.1. If university-controlled confidential, regulated, or sensitive data is discovered in publicly accessible locations or leaked to unauthorized users.

3. *Loss of Information Resources*
   3.1. Lamar University users must immediately report the loss of:
      3.1.1. University owned devices such as computers, mobile devices, storage media, hardware tokens etc., to the Property Management office.
      3.1.2. Personally owned devices such as computers, mobile devices, storage media, etc., that contained university-controlled confidential and regulated information, to the office of the ISO.

4. *Loss of Data*
   4.1. Lamar university is not responsible for:
      4.1.1. The loss of any personal data stored on university-owned information systems. For example, loss of personal pictures and documents when storage devices crash.
      4.1.2. Any potential damages that may occur from non-conformance with university policies. For example, identity theft as a result of unsecured personal devices.

5. *Return of University-owned Information Resources*
   5.1. Lamar university users are responsible for:
      5.1.1. Returning all devices issued to them after the completion of their engagement with the university. For example, computers, mobile devices, storage drives, hardware tokens, etc.

6. *Representation*
   6.1. Lamar University employees are not permitted to use university-owned information resources to:
      6.1.1. Influence the election or nomination of a person for local, state, or federal office or any similar partisan political activities.
      6.1.2. Express or represent personal views as that of the university.
      6.1.3. Intentionally access, create, store, or transmit illegal material.

Q. COMMUNICATION USAGE

Modern day communication tools such as email and Instant Messenger provide a convenient medium for exchange of information. The university invests resources to ensure official communication channels enforce security. Not all communication channels enforce the same level of protection, hence the use of appropriate channels for the exchange of confidential information is critical in maintaining privacy.

1. *Email Usage*
   1.1. The Lamar University issued email address is the official communication standard for electronic mail delivery. Lamar University users are responsible for:
      1.1.1. Monitoring their official email account.
   1.2. Lamar University email is intended for communications but not for the exchange of university-controlled confidential or regulated information. Lamar University users are required to:
      1.2.1. Use prescribed methods such as the file transfer service for such purposes.
   1.3. Lamar University maintains contracts with email providers to ensure security and privacy requirements of the university are met. Personal email providers do not guarantee the same level of security and privacy. In the event of a breach, employees take liability when using personal email for work. Lamar University employees are not permitted to:
      1.3.1. Use personal emails for university business.
      1.3.2. Forward university-controlled confidential, regulated, or sensitive emails to personal email.
      1.3.3. Auto-forward all emails to personal emails.
   1.4. Lamar University users must not:
      1.4.1. Use university email for the transmission of spam mail, chain letters, malware, phishing, personal advertisements, solicitations, or promotions.
   1.5. Lamar University is not responsible for:
      1.5.1. E-mail messages forwarded to any other email address.
      1.5.2. Users losing access to third party services when Lamar university email accounts are used to sign up or communicate with such services.
   1.6. University email accounts are not an authorized electronic repository for university

records. This policy and any administrative actions performed in the execution of the requirements therein are not a substitute for compliance with the university records retention schedule (RRS), emails that contain content governed by the university RRS should be copied to an appropriate authorized electronic repository or added to hard copy records series, as appropriate.

1.6.1. Email content that is not governed by the RRS can be deleted by the account owner upon meeting or exceeding the usefulness of the messages.

2. *Unsanctioned Communication*

2.1. Lamar University users may not use:

2.1.1. Unsanctioned communication channels like instant messenger or bulletin boards to exchange university-controlled confidential or regulated information. For example, WhatsApp, Slack, iMessage, Reddit etc.
Unsanctioned communication channels are an agreement between the provider and the individual. Hence the university cannot guarantee security or privacy to protect employees, in its use.

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. Information Systems Management Policy
E. Human Resources Policy Manual
F. Lamar Technical Control Index
G. Lamar University Records Retention Schedule

VIII. REVISION AND RESPONSIBILITY

Oversight Responsibility: IRM

Review Schedule: Every three years

Last Review Date: 06/12/2025

Next Review Date: 06/12/2028

IX. APPROVAL

Jaime Taylor - 06/20/2025

_____

President, Lamar University

Patrick Stewart - 06/20/2025

_____

IRM, Lamar University

REVISION LOG

Revision Number	Approved Date	Description of Changes
1.0	06/12/2025	Complete redraft of original policy.