POLICY LIT.3.02
APPROPRIATE USE OF INFORMATION RESOURCES

SCOPE: Faculty, Staff, Students, and Guests

1. POLICY STATEMENT

1.1. Lamar Institute of Technology (LIT) recognizes the importance of information resources and facilities to students, faculty, and staff. This policy establishes the appropriate use of information resources in order to:

1.1.1. achieve college-wide compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

1.1.2. establish prudent and appropriate practices regarding the use of information resources; and

1.1.3. educate individuals about the responsibilities they assume when using LIT's information resources.

1.2. Governing laws, regulations, and policies include:

1.2.1. Lamar Institute of Technology policies, procedures, and standards that address the use of information resources and that prohibit harassment, plagiarism, or unethical conduct.

1.2.2. Texas State University System (TSUS) policies pertaining to information resources.

1.2.3. Laws pertaining to theft, copyright infringement, insertion of malicious software into computer systems, and other computer-related crimes.

2. APPLICABILITY

2.1. This policy applies to LIT faculty, staff, students, contractors, vendors, and anyone else who uses LIT information resources.

2.2. This policy applies to all LIT information resources, regardless of where they reside.

3. GENERAL

3.1. Lamar Institute of Technology provides each of its authorized users with a computer account, known as an LIT User ID, which facilitates access to LIT's information resources. In accepting an LIT User ID or any other access ID, the recipient agrees to abide by applicable LIT policies and federal, state, and local laws. LIT reserves the right at any time to limit, restrict, or deny access to its information resources and to take disciplinary or legal action against anyone in violation of these policies or statutes.

3.2. LIT provides information resources for the purpose of accomplishing tasks related to the Institute's mission. LIT expects its faculty and staff to employ these resources as their first and preferred option for satisfying their business, research, or instructional needs.

3.3. LIT's information resources are not a public forum.

3.4. LIT considers email a significant information resource and an appropriate mechanism for official LIT communication. Lamar Institute of Technology provides official LIT email addresses and services to its students, faculty, staff, and organizational units for this purpose and to enhance the efficiency of educational and administrative processes. In providing these services, the college anticipates that email recipients will access and read LIT communications in a timely fashion.

3.5. Subject to applicable college policies and procedures, students are allowed to use the LIT's information resources for school-related purposes.

3.6. Lamar Institute of Technology employees are allowed to use the LIT's information resources in the performance of their job duties and must adhere to all applicable LIT policies and federal, state, and local laws. State law and LIT policy permit incidental personal use of institution information resources, subject to review and reasonable restrictions by the employee's supervisor.

3.7. Censorship is not compatible with LIT's goals. The college will not limit access to any information due to its content, as long as it meets the standard of legality. The college reserves the right, however, to impose reasonable time, place, and manner restrictions on expressive activities that use its information resources. Furthermore, LIT reserves the right to block or impose necessary safeguards against files and other information, such as malicious software and phishing emails, that are inherently malicious or pose a threat to the confidentiality, integrity, or availability of information resources for LIT and its stakeholders.

3.8. Lamar Institute of Technology's information resources are subject to monitoring, review, and disclosure as provided in Policy LIT.3.05 Information Security Control Standards, Section 20. Consequently, users should not expect privacy in their use of LIT's information resources, even in the case of incidental personal use.

3.9. Intellectual property laws extend to the electronic environment. Users should assume that works communicated through LIT's network and other information resources are subject to copyright laws, unless specifically stated otherwise.

3.10. The state of Texas and LIT consider information resources as valuable assets. Further, computer software purchased or licensed by the college is the property of the LIT or the company from whom it is licensed. Any unauthorized access, use, alteration,

duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas and federal statutes.

3.11. All policies that apply to college-owned computing devices (e.g., desktop computers, laptop computers, or mobile devices) used on campus also apply to those used off-campus (e.g., college-owned home-based computers, mobile devices, or laptop use while travelling), including restrictions on use as listed in Section 4 of this policy.

4. INAPPROPRIATE USES OF INFORMATION RESOURCES

4.1. The following activities exemplify inappropriate use of the LIT's information resources. These and similar activities are strictly prohibited for all users:

4.1.1. Use of LIT information resources for illegal activities or purposes. The institution will deal with such use appropriately and will report such use to law enforcement authorities. Examples of illegal activities or purposes include unauthorized access, intentional corruption or misuse of information resources, theft, and child pornography.

4.1.2. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the LIT's information resources.

4.2. The abuse of information resources, including any willful act that:

4.2.1. endangers or damages any specific computer, software, hardware, program, network, data, or the system as a whole, whether located on campus or elsewhere on the global Internet;

4.2.2. creates or allows a computer malfunction or interruption of operation;

4.2.3. injects malicious software into an information system;

4.2.4. sends a message with the intent to disrupt Institute operations or the operations of outside entities;

4.2.5. produces output that occupies or monopolizes information resources for an unreasonable time period to the detriment of other authorized users;

4.2.6. consumes an unreasonable amount of college-controlled communications bandwidth to the detriment of other authorized users; or

4.2.7. fails to adhere to time limitations that apply at computer facilities on campus.

4.3. Use of LIT information resources for personal financial gain or commercial purpose.

4.4. Failure to protect a password or LIT User ID from unauthorized use.

4.5. Falsely representing one's identity through the use of another individual's LIT User ID or permitting the use of an LIT User ID and password by someone other than their owner.

This restriction also applies to Personal Identification Numbers (PINs), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes.

4.6. Successful or attempted unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained on any LIT owned or controlled information resource.

4.7. Installing any software on college-owned information resources without Information Technology Services department approval.

4.8. Unauthorized duplication, use, or distribution of software and other copyrighted digital materials (including copyrighted music, graphics, videos, etc.). All software and many other digital materials are covered by some form of copyright, trademark, service mark, license, or agreement with potential civil and criminal liability 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, must apply.

4.9. Participating or assisting in the deliberate circumvention of any security measure or administrative access control that pertains to Institute information resources.

4.10. Using LIT information resources in a manner that violates other college policies (including those found in the Student Handbook), such as racial, ethnic, religious, sexual, or other forms of harassment.

4.11. Using LIT information resources for malicious activities such as phishing or the transmission of spam mail, chain letters, malicious software (e.g., viruses, worms, or spyware).

4.12. Using LIT information resources for personal advertisements, solicitations, or promotions.

4.13. Modifying any wiring or attempting to extend Institute owned or controlled networks beyond the port (e.g., adding hubs, switches, wireless access points, or similar devices) in violation of Policy LIT.3.05 Information Security Control Standards, Section19.

4.14. Using LIT's information resources to affect the result of a local, state, or national election or to achieve any other political purpose (consistent with Texas Government Code §556.004).

4.15. Using LIT's information resources to state, represent, infer, or imply an official LIT position without appropriate authorization.

4.16. Unauthorized network scanning, foot printing, reconnaissance, or eavesdropping on information resources for available ports, file shares, or vulnerabilities.

4.17. Unauthorized alteration or relay of network traffic (e.g., man in the middle attacks).

4.18. Employee use of computing devices not under the direct ownership of the employee or LIT (e.g., public-use computers in libraries, hotels, and other locations) to access Confidential or Sensitive data stored on Institute information resources.

4.19. The following restrictions apply to incidental use of LIT information resources:

4.19.1. Incidental personal use of information resources is restricted to LIT-approved users; it does not extend to family members or other acquaintances.

4.19.2. Incidental use must not result in direct cost to the college.

4.19.3. Incidental use must not interfere with the normal performance of an employee's work duties.

5. RESPONSIBILITIES OF USERS

5.1. Each user shall utilize LIT information resources responsibly and respect the needs of other users.

5.2. In keeping with LIT's core values, all use of its information resources should reflect high ethical standards, mutual respect, and civility.

5.3. Users are responsible for any activity that takes place using their account.

5.4. Users must report any suspected weaknesses in computer security, any incidents of possible abuse or misuse, or any violation of this agreement to the Information Technology Services department and/or the ISO immediately upon discovery.

5.5. Unit heads and supervisors must report ongoing or serious problems regarding the use of LIT information resources to the Information Technology Services department.

5.6. Each user shall immediately notify the Information Technology Services department and/or the ISO of the loss of any fixed or portable storage device or media, regardless of ownership, that contains college data. (See Policy LIT.3.05 Information Security Control Standards, Section 12.)

6. ACCESS TO INSTITUTE INFORMATION RESOURCES BY AUDITORS

6.1. Consistent with Texas State University System (TSUS) policies, the TSUS director of Audits and Analysis and auditors reporting to them, either directly or indirectly, while in the performance of their assigned duties, shall have full, free, and unrestricted access to all LIT information resources, with or without notification or consent of the assigned owner of the resources. This includes personal information stored on LIT information

resources. The college shall afford this access consistent with Policy LIT.3.05 Information Security Control Standards, Section 9.

6.2. The college shall provide state, federal, and other external auditors with access to LIT information resources with prior approval by the IRM and proper notification of the Office of Internal Audit. Lamar Institute of Technology shall afford this access consistent with Policy LIT.3.05 Information Security Control Standards, Section 9.

7. CONSEQUENCES FOR FAILURE TO ADHERE TO THIS POLICY

7.1. Failure to adhere to this policy may lead to the revocation of a user's LIT User ID, suspension, dismissal, or other disciplinary action by the college, as well as referral to legal and law enforcement agencies.

7.2. Statutes pertaining to the use of LIT information resources:

7.2.1.1. The Federal Family Educational Rights and Privacy Act (FERPA) – restricts access to personally identifiable information from students' education records.

7.2.1.2. 1 Tex. Admin. Code §202 – establishes information security requirements for Texas state agencies and public institutions of higher education.

7.2.1.3. Texas Penal Code, Chapter 33: Computer Crimes – specifically prohibits unauthorized use of LIT computers, unauthorized access to stored data, or dissemination of passwords or other confidential information to facilitate unauthorized access to LIT's computer system or data.

7.2.1.4. Texas Penal Code, §37.10: Tampering with Governmental Record – prohibits any alteration, destruction, or false entry of data that impairs the validity, legibility, or availability of any record maintained by LIT.

7.2.1.5. United States Code, Title 18, Chapter 47, §1030: Fraud and Related Activity in Connection with Computers – prohibits unauthorized and fraudulent access to information resources, accessing a computer to obtain restricted information without authorization; altering, damaging, or destroying information on a government computer without authorization; trafficking in passwords or similar information used to gain unauthorized access to a government computer; and transmitting viruses and other malicious software.

7.2.1.6. Copyright Law, 17 U.S.C. §101-1332 – forms the primary basis of copyright law in the United States, as amended by subsequent legislation. The Law spells out the basic rights of copyright holders and codifies the doctrine of fair use.

7.2.1.7. Digital Millennium Copyright Act (DMCA), 17 U.S.C. §512 as amended and 28 U.S.C. §4001 – criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. The Act amended Title 17 of the United States Code to extend the reach of copyright, while limiting the liability of internet service providers (like LIT) for copyright infringement by their users, provided the service provider removes access to allegedly infringing materials in response to a properly formed complaint.

7.2.1.8. Electronic Communications Privacy Act (U.S.C., Title 18) – prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

7.2.1.9. Computer Software Rental Amendments Act of 1990 – deals with the unauthorized rental, lease, or lending of copyrighted software.

7.2.1.10. Texas Government Code §556.004 – prohibits using state resources or programs to influence elections or to achieve any other political purpose.

7.2.1.11. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R 164 – sets security management requirements and broad management controls to protect the privacy of patient health information.

7.2.1.12. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §3541 – requires every federal agency to develop, document, and implement an agency-wide information security program. The law was amended by FISMA 2010, which changed the focus from paperwork compliance to continuous monitoring and threat mitigation.

Related Procedures:

Relevant Forms/Documents:

Relevant TSUS Policies/Forms/Documents: TSUS Sexual Misconduct Policy and Procedures; TSUS Rules and Regulations Chapter III, Paragraph 7.(10)3

Relevant Statutes: Computer Software Rental Amendments Act of 1990 ; Copyright Law, 17 U.S.C. §101-1332, 18 U.S.C. §2318-2323; Digital Millennium Copyright Act (DMCA), 17 U.S.C. §512 as amended and 28 U.S.C. §4001; Electronic Communications Privacy Act (U.S.C., Title 18) ; Federal Family Educational Rights and Privacy Act (FERPA); Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §3541; Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R 164; United States Code, Title 18, Chapter 47, §1030: Fraud and Related Activity in Connection with Computers; 1 Tex. Admin. Code §202; Texas Government

Code §556.004; Texas Penal Code, Chapter 33: Computer Crimes; Texas Penal Code, §37.10: Tampering with Governmental Record

Relevant SACSCOC Standards:

Document History:
Adopted:
Reviewed:
Revised: September 2025