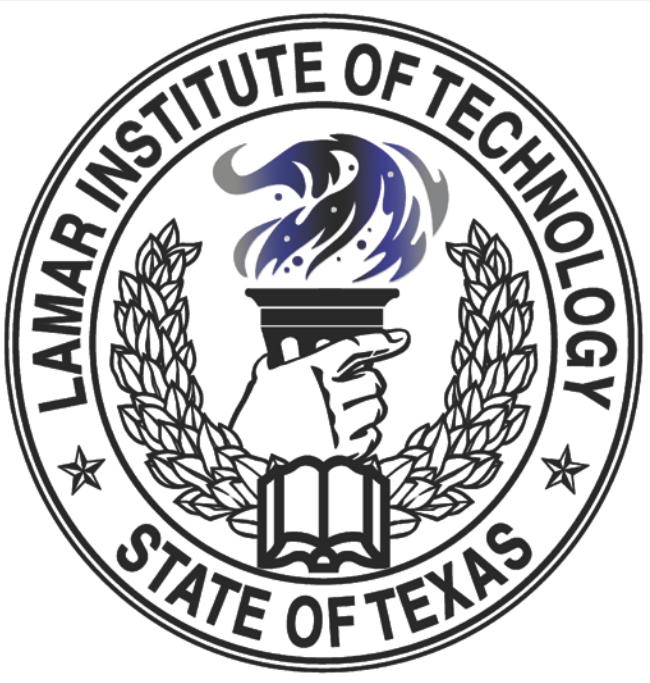
Information Security:
Appropriate Use of Information Technology



Technology Services

1/4/2013

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Appropriate Use of Information Technology

The purpose of this session is to:

- To establish prudent and acceptable practices regarding the use of information resources
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

General Guidelines and Principles

- LIT provides each of its authorized users with a computer account, known as a LIT user ID, which facilitates access to the LIT's information resources.

- Applicable LIT policies and procedures include all LIT policies and procedures that address the usage of LIT information resources.

- LIT provides information resources for the purpose of accomplishing tasks related to the LIT's mission.

General Guidelines and Principles (Cont.)

- LIT considers e-mail a significant information resource and an appropriate mechanism for official LIT communication. LIT provides official e-mail addresses and services to its students, faculty, staff, and organizational units for this purpose and to enhance the efficiency of educational and administrative processes.

- Employees of LIT are allowed to use LIT's information resources in the performance of their job duties as long as they adhere to all applicable policies and statutes. Incidental personal use of information resources by an employee is permitted, subject to review and reasonable restrictions by the employee's supervisor.

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Inappropriate Uses of Information Resources

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

- Use of LIT information resources for illegal activities or purposes. Illegal activities or purposes include unauthorized access, intentional corruption or misuse of information resources, theft, obscenity, and child pornography.

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

Inappropriate Uses of Information Resources (Cont.)

- The abuse of information resources includes any willful act that: 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.

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

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

Inappropriate Uses of Information Resources (Cont.)

- Falsely representing one's identity through the use of another individual's LIT ID or permitting the use of a ID and password by someone other than their owner.
- Unauthorized use of or access to any electronic file.
- Unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained on any electronic file, program, network, web page, or LIT hardware or software.

Inappropriate Uses of Information Resources (Cont.)

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

- Using LIT information resources in a manner that violates other LIT policies, such as racial, ethnic, religious, sexual or other forms of harassment.

- Using LIT information resources for the transmission of spam mail, chain letters, malicious software (e.g., viruses, worms, or spyware), or personal advertisements, solicitations or promotions.

Inappropriate Uses of Information Resources (Cont.)

- Using LIT's information resources to affect the result of a local, state, or national election or to achieve any other political purpose.

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

Responsibilities of Users

- Each user shall utilize LIT information resources responsibly and respect the needs of other users.
- Each person is responsible for any usage of his or her LIT ID. Users must maintain the confidentiality of their passwords.
- A user must report any abuse or misuse of information resources or violations of this policy to their department head or to the Director of Computer Services.

Responsibilities of Users (Cont.)

- When communicating with others via LIT information resources (e. g., e-mail), a user's communications should reflect high ethical standards, mutual respect and civility.

- Users are responsible for obtaining and adhering to relevant, acceptable network use policies.

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Liabilities for Failure to Adhere to This Policy

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

Related Statutes

- Texas Administrative Code, Title 1, Part 10, Chapter 202 - Regulations from the Department of Information Resources establishing requirements for State agencies regarding computer security.

- Texas Penal Code, Chapter 33: Computer Crimes - Texas law pertaining to computer crimes. This statute 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 the LIT's computer system or data.

- 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.

Related Statutes (Cont.)

- United States Code, Title 18, Chapter 47, § 1030: Fraud and Related Activity in Connection with Computers - Federal law specifically pertaining to computer crimes. Among other stipulations, prohibits unauthorized and fraudulent access to information resources.

- Computer Fraud and Abuse Act (Part of Title 18, Chapter 47, U.S.C. § 1030) - Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

Related Statutes (Cont.)

- The Computer Abuse Amendments Act of 1994 (Part of Title 18, Chapter 47, U.S.C. § 1030) - Expands the Computer Fraud and Abuse Act of 1986 to address the transmission of viruses and other harmful code.

- Federal Copyright Law - Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.

Related Statutes (Cont.)

- Digital Millennium Copyright Act (DMCA) - Signed into law on October 20, 1998, as Public Law 105-304. Created to address the digitally networked environment, the DMCA implements the World Intellectual Property Organization (WIPO) Internet Treaties; establishes safe harbors for online service providers; permits temporary copies of programs during the performance of computer maintenance; and makes miscellaneous amendments to the Copyright Act, including amendments that facilitate Internet broadcasting.

Related Statutes (Cont.)

- 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.

- Computer Software Rental Amendments Act of 1990 - Deals with the unauthorized rental, lease, or lending of copyrighted software.

- Texas Government Code § 556.004 - Prohibits using state resources or programs to influence elections or to achieve any other political purpose.