# Information Security:
# Roles, Responsibilities, and Data Classification

LAMAR INSTITUTE OF TECHNOLOGY

STATE OF TEXAS

## Technology Services

1/4/2013

# Roles, Responsibilities, and Data Classification

The purpose of this session is to:

- Establish that all individuals are accountable for their use of LIT information.
- Identify information Owners, Custodians, and User roles to clearly distinguish the parties responsible and accountable for that LIT information.

## Roles, Responsibilities, and Data Classification (Cont.)

- Establish that information that is sensitive or confidential must be protected from unauthorized access or modification.

- Establish that security awareness of employees must be continually emphasized and reinforced at all levels of management.

# General Guidelines

- Information resources residing at LIT are strategic and vital assets that belong to the people of Texas.

- All individuals are accountable for their use of LIT information resources.

- Information that is Sensitive or Confidential must be protected from unauthorized access or modification.

# Information Owners

- LIT delegates specific ownership responsibilities to those with day-to-day oversight of information assets.
  - For example, individual departments are owners of the information located in the departmental file shares in the LIT data center.
- Owners have been designated for data assets based upon the general subject matter of the data.
  - For example, Human Resources is the owner of staff and faculty employee information.

# Information Custodians

- Custodians provide information asset services to both owners and users.

- A custodian may be a person, a team, or a department such as Technology Services.

- A custodian could be a third party provider of information resources. (i.e. website or application hosting provider)

# Information Custodians (Cont.)

Regardless of how the role is filled, custodians are expected to:

- Assist the owner(s) in identifying cost-effective controls along with monitoring techniques and procedures for detecting and reporting control failures or violations

- Implement the controls and monitoring techniques and procedures specified by the owner(s)

- Provide and monitor the viability of physical and procedural safeguards for the information resources

# Information Users

- Users of information resources shall use those resources for defined purposes that are consistent with their institutional responsibilities.

- Users are expected to comply with LIT published security policies and procedures, as well as with security bulletins and alerts in response to specific risks or threats.

- The use of LIT information resources implies that the user has knowledge of and agrees to comply with LIT policies governing such use.

# Data Classification

- Owners of LIT information assets shall classify the information as public, sensitive, or confidential, according to its need for confidentiality.

- The information’s owner should ensure that disclosure controls and procedures are implemented and followed to afford the degree of protection required by the assigned classification.

# Data Classification (Cont.)

Information shall be assigned one of the following 3 classifications:

- Public - Advertising and Marketing Literature
- Sensitive - Employee Records, Voicemail, and Memos
- Confidential - Credit Card Information and Social Security Numbers

# Data Classification (Cont.)

## Public Information

- Public information is by its very nature designed to be shared broadly, without restriction, at the complete discretion of the owner.
  - Examples of public information include: advertising and marketing literature, degree program descriptions, course offerings and schedules, campus maps, job postings, press releases, descriptions of LIT products and services, and certain types of unrestricted directory information.

# Data Classification (Cont.)

## Sensitive Information

- Sensitive information can be both public and confidential. Sensitive information may be deemed public if subject to provisions of the Texas Public Information Act.
  - Examples of sensitive information include: some employee records, departmental policies and procedures that may reveal protected information, the contents of e-mail, voicemail, and memos, information covered by non-disclosure agreements, and donor information.

# Data Classification (Cont.)

## Confidential Information

- Confidential information is information that is exempt from disclosure requirements under the provisions of applicable state or federal law.
  - Examples of confidential information include: student education records as defined under FERPA, credit card and financial account information, social security numbers, driver license numbers, personally identifiable medical records, crime victim information, and access control credentials (e.g., PINs and passwords).

# Additional Information

- Sensitive or confidential information must not be transmitted in unencrypted form.  Either the information itself must be encrypted prior to transmission or an encrypted connection must be established and maintained for the duration of the transmission.

- Owners, custodians and users must immediately report suspected information resources security incidents to Technology Services Help Desk at (409) 839-2074, or email to helpdesk@lit.edu.