UNT | SYSTEM
IT Shared Services

Information Technology Security and Compliance Requirements for Departments, Managers, and Supervisors

Introduction

The information provided in this resource will aid departments in establishing appropriate compliance practices for information and resources under their control or management. These guidelines provide information regarding best practices for acquiring, using, and managing information and resources.

The information provided in this guide is based on compliance regulations, policies, standards, and best practices. It is recommended that departments check this information regularly as it may be updated to reflect changes.

Use of Computing Resources

The University of North Texas provides computer resources for the purpose of accomplishing tasks related to the University's mission. Students, including registered students as well as incoming students who have paid their fees, shall be allowed to use the University's computer resources for school-related and personal purposes. An employee of the University shall be allowed to use computer resources in accordance with this and other applicable University policies. Incidental personal use of computer resources by employees is permitted, subject to review and reasonable restrictions by the employee's supervisor; adherence to applicable University policies and state and federal law; and as long as such usage does not interfere with the employee's accomplishment of his or her job duties and does not result in any additional costs to the University.

Users of the University's computer systems should be aware that computer use may be subject to review or disclosure in accordance with the Texas Public Information Act and other laws; administrative review of computer use for security purposes or in regard to a policy or legal compliance concern; computer system maintenance; audits and as otherwise required to protect the reasonable interests of the University and other users of the computer system. Anyone using the University's computer systems expressly consents to monitoring on the part of the University for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity, University administration may provide that evidence to law enforcement officials.

Protecting Information and Resources: The Basic Premises of Information Security

Information security is based on three premises: ensuring the confidentiality, integrity and availability of information and resources. It is everyone's responsibility to ensure that information and resources are protected per these premises.

Confidentiality- protecting information from unauthorized disclosure

Integrity- protecting information from unauthorized modification

Availability- ensuring information resources may be accessed and utilized when needed

Security Roles for Departments and Department Heads

There are various categories of users that have unique responsibilities for ensuring the security of information and resources. Departments and department heads act in at least one of two roles. They are considered **custodians** or **owners of information**. Departments that use records that were created or owned by other units act as custodians of information. For example, the Registrar is the owner of student information, and may grant permission to a department to use student records for business purposes. Departments that create original records act as owners of information. A department head is considered the information owner of records created by the department that they manage.

Departments must obtain written permission from information owners to use data. This is required for each unique information request.

The role of a department head acting as an information owner is to accept ownership of records, identify and confirm controls, establish access requirements, and assign custody of information.

A department head acting as a custodian is required implement the controls defined by the owner and must adhere to requirements for obtaining access to information or resources.

Security Roles for Managers and Supervisors

Managers and supervisors should ensure that employees are aware of their responsibilities for protecting information and resources. Employees should complete security awareness training and also refer to the UNT System Information Security Handbook for information about the security of information and resources. In addition, managers and supervisors are responsible for ensuring that computer access is reviewed, modified, or terminated when an employee's employment status changes (e.g., transfers, promotions, leave of absence, terminations, etc.).

Handling Confidential or Sensitive Information

Federal and state laws include special regulations for handling information that is deemed confidential, sensitive, or personally identifiable. These types of information include health, student, employee, private donors, library records, financial data (credit cards and bank account information), export controlled data, research data, and computer vulnerability assessment reports. This information must be protected according to legal and contractual obligations. Data that fall into the categories listed below must be encrypted while in transit, if stored on portable devices, and if stored a non-UNT owned system.

- Health information
- Student records
- Employee information
- Private donor information
- Library records
- Financial data are protected by the following:
- Export Controlled data and technology
- Research data

Publishing Information about Students, Faculty, or Staff

Certain types of information about students and employees are restricted from public disclosure, and as such may not be disclosed on websites or in other public forums, or to entities that are not contractually obligated to protect the information. This information is generally confidential, sensitive, or considered personally identifiable information. It may not be obvious what is permissible to publish (e.g., under certain conditions, a student's name cannot be published). Make sure you are aware of legal regulations and UNT policies regarding publication of information BEFORE it is published.

In addition, internet websites or mobile applications that will be used to process confidential information must undergo a security vulnerability assessment and penetration test before the website or mobile application can be deployed. This is required to ensure that institutions protect the privacy of individuals. Contact the information security officer for your campus for assistance. At minimum, the following must be submitted to your information security officer for review:

- The architecture of the website or application;
- The authentication mechanism for the website or application; and
- The administrator level of access to data included in the website or application.

General Security Checklist

- Departments should follow best practices for handling information. Maintain knowledge and implement the protection requirements for information or data that you use.
- Ensure that faculty and staff attend security awareness training prior to handling information, and must also take refresher courses annually.
- Ensure that physical security measures are in place, e.g., restrict access to areas where confidential or sensitive information is stored, protect paper documents from authorized viewing, etc.
- Work with your departmental or college network manager to ensure that your workstation and other computer resources are properly secured and licensed.
- Maintain awareness and foster an environment promoting security among employees.
- Develop business continuity plans in the event that information or resources become unavailable.
- Be aware of intellectual property and copyright requirements for resources.
- Use the resources listed in this guide to make sure you are adequately protecting the data and resources entrusted to you.
- Understand your role as an information owner or custodian.
- Report suspicious computing activities to your IT manager.
- Modify or remove computing access for employees when their employment status changes (e.g., transfers, promotions, leave of absence, terminations, etc.)
- Obtain permission from information owners to use data.
- Consult with the department that is responsible for approving the use of payment processing (in accordance with PCI-DSS) prior to implementing payment processing services.
- Contact the information security officer (security@untsystem.edu) to ensure that a vulnerability assessment and penetration test have been conducted before deploying a website or mobile application.
- For the full list of custodial responsibilities, please read your institution's information resources or computing policies.

General Information about Outsourcing Information Technology or Support to a Third-Party

Departments that seek to acquire software, hardware, applications, resources or other third-party solutions that are not currently provisioned by a department at your institution must consider the risks associated with outsourcing prior to acquisition. As most outsourcing arrangements require use of one or more types of institutional data, may support payment processing, or may require the collection of information from individuals, departments must seek and obtain permission from UNT information owners and must also ensure that a security assessment is undertaken to determine risks associated with the arrangement.

Departments that wish to outsource payment processing (i.e., credit card processing) must consult with the department that is responsible for approving

payment processing (in accordance with PCI-DSS) prior to implementing payment processing services. Departments that enter into outsourcing arrangements must accept responsibility for the risks associated with outsourcing.

Before Acquiring Software or Outsourcing Information Technology Support to a Third-Party

1. Develop a project plan.
2. Ensure that the project plan allows at least three scheduled weeks that can be devoted to IT planning, review, coordination or support prior to acquisition, negotiation or other purchase of the resource.
3. Contact your IT liaison and make him/her aware of your needs. In addition, do the following:
    a. Make contact with appropriate information technology units that will be needed to support the project, i.e., Project Management Office, department responsible for approving PCI-DSS, Information Security, Enterprise Application Support (for programming and development support), Data Communications, and other applicable IT units;
    b. With the assistance of your IT manager complete security risk assessment questionnaires and non-disclosure agreements, where appropriate. Departments typically obtain and complete of all of the following:
        i. Systems Acquisition Survey (required);
        ii. Non-disclosure Agreement, NDA (third-party and CFO will sign this agreement); and
        iii. Schedule or request a review of information technology compliance and security requirements for the project.
    c. Submit the completed documents to your IT manager and the UNT System IT Compliance office.
4. Understand your role-- Are you an information owner or custodian?
5. Seek permission from information owner(s) to use data.
6. Obtain permission from the department that is responsible for approving payment processing (in accordance with PCI-DSS) prior to implementing payment processing services.
7. Contact the information security officer (security@untsystem.edu) to ensure that a vulnerability assessment and penetration test have been conducted before deploying a website or mobile application.
8. Obtain appropriate legal documents or agreements that ensure a contractual relationship between your institution and a third-party.
9. Ensure that legal documents are signed by all authorized parties prior to provisioning access to the resource
10. Ensure that security or compliance recommendations are applied.

Special Access Considerations for Third-Parties or Other Non-UNT Parties
After contractual obligations and planning for IT management is complete, departments that seek to allow external parties (such as vendors, consultants, or other external parties) to access institutional resources must work with their IT liaison to conduct specify security requirements related to accessing appropriate resources. Third-parties that wish to obtain access to ITSS (Information Technology Shared Services) systems must obtain written approval from the Information Security Officer or designee, and also accept their responsibilities for ensuring the security of resources for which access is approved. This will require completion of security clearance forms that are available from the Information Security Officer.

Where to Find Addition Information about Security and Compliance
Additional information about security and compliance can be found on the Information Security website, http://security@untsystem.edu.

Where to Seek Assistance

- Locate Your IT Manager
- Send Email to ITCompliance@untsystem.edu
- Report a Security Incident

Planning Resources
Business Continuity Planning

Security Awareness Training
Information Security Training

Computing Policies, Standards and Handbook
Information Technology Policies
UNT System Information Security Handbook

Privacy and Protection Laws, Regulations and Standards
Texas Administrative Code 202, Information Security Standards
Texas Government Code 2054.517
Family Educational Rights and Privacy Act (FERPA)
Health Information and Portability Accountability Act (HIPAA)
Payment Card Industry Data Security Standards (PCI-DSS)
Digital Millennium Copyright Act (DMCA)
Texas Public Information Act
Gramm Leach Bliley Act (GLBA)
Texas Identity Theft Enforcement and Protection Act

Federal Trade Commission Rule Red Flags Rule

U.S. Department of Commerce Export Administration Regulations (EAR)
U.S. Department of Treasury Office of Foreign Assets Control (OFAC)
U.S. Department of State International Traffic in Arms (ITAR)