UNT SYSTEM

IT SHARED SERVICES

Information Owner Training

May 27, 2015

IT Shared Services

itss-securitytraining@untsystem.edu

Why me?

The Texas Administrative Code requires the institution to identify information owners and document their responsibilities.

You were identified by representatives of the Shared Services Operations Committee as an information owner. Committee members include:

- Chief Internal Auditor
- General Counsel
- Campus Provosts and Vice Chancellor for Academic Affairs and Student Success
- Campus Chief Financial Officers and Vice Chancellor for Finance
- Vice Chancellor for Administration

Resources for Information Owners

- All information in this presentation can also be found in more detail in the Information Ownership Guide
- Additional resources are located on the Information Ownership Website

Information owners can help prevent data loss

- UNT Security Incidents and Data Breaches
  - 12 data breach incidents from 2005-2015, 10 were due to inadvertent exposure by UNT employees
  - All involved the loss of personally identifiable information
  - Maximum loss of 36,000 records in a single incident
- Other universities have experienced breaches
  - University of North Carolina Chapel Hill- 350,000 student records were released on the internet in 2012
  - University of Nebraska Lincoln- 650,000 student and applicant records were hacked by a UNL student
  - Auburn University- made public information regarding 370,000 students in 2015

Security Roles

- *Information Owners* - are individuals with operational authority for specified information and who are responsible for authorizing the controls for the generation, collection, processing, access, dissemination, and disposal of that information

- *Custodians* – are responsible for implementing the information owner-defined controls and access to an information resource

- *Users* - are individuals or an automated application authorized to access an information resource

- *Information Security Officer* - provides guidance and assistance to information owners and others concerning security roles and responsibilities

Information Owners' Areas of Responsibility

Information Owners set the tone for a security-minded environment.

1. Know how your data is categorized
2. Manage Access to data
3. Work with Custodians
4. Work with ISO

Responsibility 1:

Know How Data is Categorized

Categories of Information

Category I – Protected information: E.g. social security numbers, credit card information, student education records.

Category II – Should be controlled before release: E.g. some directory Information

Category III – Public information available for release.

Categories of Information

- All information has been categorized.
- Categorization and ownership documentation is posted on the UNT System Information Ownership website.

Information (Data)	Ownership Level	* Information Category	UNT	UNT Health Science Center	UNT Dalllas	UNT System Administration	UNT Dallas College of Law
Academic Information (student degree plans, advising information, etc.)	UNT System or Institution	Confidential Information (Category I)	Provost	Provost	Provost	N/A	Dean
Applicant Admission Information	UNT System or Institution	Confidential Information (Category I)	VP for Enrollment Management	Provost	VP for Enrollment Management	N/A	Dean
Asset Information	UNT System or Institution	Public Information (Category III)	Chief Financial Officer	Chief Financial Officer	Chief Financial Officer	Vice Chancellor for Finance	N/A
Audit Information	UNT System	Confidential Information (Category I)	N/A	N/A	N/A	Chief Internal Auditor	N/A
Budget Information	UNT System or Institution	Public Information (Category III)	Institution Budget Officer	Institution Budget Officer	Institution Budget Officer	Institution Budget Officer	Institution Budget Officer

Chart is sample data only

Responsibility 2:

Manage Access to Data

Manage Access to Data

1. Grant approval authority to individuals designated to act on your behalf (e.g. ACEs)
2. Document your approval and the type of access granted to designated representative(s) and other individuals that you authorize to use information.
3. Review and revise access lists periodically
   - *Reviews should be conducted at least annually*
   - *Reviews should occur more frequently depending on the importance of the data*
   - *Reviews should consider changes in employment*

Responsibility 3:

Work With Custodians

Work with Custodians

1. Formally assign custody of data to custodians
2. Ensure custodians understand security controls and procedures that you authorize
3. Provide authority to custodians to implement procedures defined by you

Work with Custodians - Formally Assign Custody of Data

- Custodians may already be assigned their responsibilities based on current practices and procedures
- Some examples of custodians are:
  - IT Shared Services
  - ACEs
  - IT Managers and support staff
  - Business Unit employees

Know who your custodians are!

Responsibility 4:

Partner with the Information Security Officer

Work with the Information Security Officer (ISO)

The Information Security Officer for the UNT System, UNT and UNT Dallas is Charlotte Russell. The Information Security Officer for HSC is Anthony Tissera.

1. Cooperate with the ISO by following the UNT System Information Security Handbook
2. Work with the ISO in regard to granting security exceptions
3. Participate in Risk Assessments with the ISO

Summary

What do I need to do?

- Read the Information Ownership Guide
- Read the UNT System Information Security Handbook
- Establish procedures for documenting and reviewing custodianship
- Work with the Information Security Officer to complete risk assessments and when requesting security exceptions
- Ensure data security requirements are met through people, processes and technology
- Convey that security is everyone's job

Resources

- UNT System Information Ownership Guide
- UNT System Information Ownership Website
- UNT System Information Security Handbook
- UNT System Information Security Regulation
- Texas Administrative Code, Section 202

For additional assistance, e-mail:

itss-securitytraining@untsystem.edu