Information Ownership Guide

Scope

This document applies to all information owners at the University of North Texas System member institutions and System Administration.

Purpose

The University of North Texas System has established an Information Security Regulation and Handbook, based upon Texas Administrative Code requirements, which states that information owners must protect their data. This Information Ownership Guide sets forth the responsibilities of information owners.

Information Owners set the tone for a security-minded environment. Security is comprised of the behaviors of people, business processes, and technological controls. It is the Information Owner's role to convey that security is everyone's job and to ensure security strategies are in place at all times.

Roles

Security roles include information owners, custodians, and users. Guests, contractors, consultants, and vendors can serve as custodians and act as users as well.

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

Custodians are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by information owners for performing tasks also act as custodians of the information and are responsible for maintaining the security of the information.

The Custodian is the person responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the System Administration or an Institution.

Users are an individual or automated application authorized to access an information resource in accordance with the information owner-defined controls.

Information Security Officer provides guidance and assistance to information owners and others concerning security roles and responsibilities. The Information Security Officer is appointed by the head of each institution and is responsible for developing and administering the operation of an information security program.

Last update: 9/25/2017

Procedures

Information owners or their designated representative(s) are responsible for knowing how data is classified, managing access to data, working with the custodians who have access to the owner's data, and working with the Information Security Officer to complete security exceptions and participate in risk assessments. Information Owners can delegate tasks, but not accountability.

Classify Data

The UNT System Information Security Regulation (Regulation 06.001) establishes Information classification categories. All UNTS information falls into one of three categories.

Category I

Information that requires protection from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, and judicial requirements), legal agreement, or information that requires a high degree of confidentiality, integrity, or availability.

Category I information must be identified, documented, and protected.

Examples include: financial aid information, health or medical information, computer account information, social security numbers, and emplids.

Category II

Information that is proprietary to an institution or has moderate requirements for confidentiality, integrity, or availability.

Examples include: grants information, donor information, patron information, some payroll information.

Category III

Information with low requirements for confidentiality, integrity, or availability and information intended for public release as described in the Texas Public Information Act.

Examples include information subject to release under public information requests.

The Shared Services Operation Committee has classified all UNT System information.[1] A list of owners and classification by type of information is described in the *Categorization and Ownership Documentation.*

Manage Access to Data

Information owners or their designated representative(s) must manage access to data by approving requests for access, documenting individuals with access, and reviewing access lists periodically.[2] Owners should limit access to data to those with an actual business need by using established criteria to determine necessity. Information owners must maintain a list of their designated representative(s) and all individuals with access and must periodically review this list. Information Owner or their delegates should conduct reviews at least annually and after major changes. Reviews should also occur more frequently depending on the importance of the data. Reviews should consider changes in employment.

If an individual who no longer needs access is on the list, owners must work to revoke their access.

For most services within EIS, the Access Control Executives (ACEs) have the ability to retrieve information about who can access data. IT Shared Services can provide information owners with a list of their ACEs. Information owners should work with their ACEs to request data access details. Similar abilities may exist within other applications as well. Contact your service provider to determine if this capability exists.

Work with Custodians
Information owners must also formally assign custody of data.[3] Groups of UNT System custodians are; are ACEs, IT Shared Services, and the Enterprise Applications team. Owners must ensure custodians follow proper procedures regarding data handling.[4] Owners must also provide authority to their custodians to implement owner-defined controls and procedures.[5]

Promoting a culture of security is important when working with custodians and designated representative(s). For example, by completing security awareness training this encourages custodians to do the same.

Work with the Information Security Officer
Information Owners should collaborate with the Information Security Officer (ISO) as needed for security exceptions.[6] In the event that information security controls required by the UNTS information security program cannot be met, information owners must work with the ISO to determine if an exception is possible. Owners are responsible for justifying, documenting, and being accountable for exceptions to security controls. Information owners coordinate and obtain approval for exceptions to security controls with the ISO.

Owners must also participate in risk assessments.[7] These include annual risk assessments of enterprise resources required by state law and the Information Security Regulation as well as additional risk assessments as needed. During the annual risk assessment, owners will assist the ISO with risk management decisions for their areas.

Information owners must cooperate with the ISO by following the Information Security Handbook.[8]

Resources

UNT System Information Security Users Guide
UNT System Information Security Team
UNT System IT Policies and Standards
UNT System Information Ownership Assignments

References

Texas Administrative Code 202.72
UNT System Information Security Handbook
UNT System Information Security Regulation
UNT System Administration Information Security Policy
UNT Information Resources Security Policy
UNT Dallas Information Security Policy
UNT (under review)

Last update: 9/25/2017

[1] Texas Administrative Code §202.72(1)(A)
[2] Texas Administrative Code §202.72(1)(B)
[3] Texas Administrative Code §202.72(1)(C)
[4] Texas Administrative Code §202.72(1)(E)
[5] Texas Administrative Code §202.72(1)(F)
[6] Texas Administrative Code §202.72(1)(G)
[7] Texas Administrative Code §202.72(1)(H)
[8] Texas Administrative Code §202.72(1)(D)