UNT SYSTEM™

INFORMATION OWNERSHIP GUIDE

Purpose

The UNT System Enterprise (Enterprise) is committed to protecting the confidentiality, integrity, and availability of its information. To ensure the protection of Enterprise information, Information Owners are required to adhere to this guide when fulfilling their obligations for Enterprise information under their authority, in accordance with Texas Administrative Code § 202.72. This guide serves as the Enterprise standard for Information Owners and offers guidance for the protection of Enterprise information under their authority.

Scope

This guide applies to all Information Owners and Information Stewards of the Enterprise.

Definitions

1. Custodian. Custodian means a person responsible for implementing the Information Owner-defined controls and access to information and information resources. 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. Custodians may include employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the System Administration and Institutions.
2. Chief Information Security Officer (CISO). Chief Information Security Officer (CISO) means the agency official responsible for developing and administering the operation of the Information Security Program, providing leadership, strategic direction, and coordination for the UNT System Enterprise Information Security Program, including issuing policies, standards, procedures, and guidelines.
3. Delegation of Authority. Delegation of Authority in this guide means the specific written transfer of authority from an Information Owner (delegator) to an Information Steward (delegate).
4. Information Owner. Information Owner means a person with operational authority for specified information and who is responsible for authorizing the controls for generation, collection, processing, access, dissemination, and disposal of that information.

5. Information Resources. Information Resources means the procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information and associated personnel including consultants and contractors.
6. Information Steward. Information Steward means a delegate of the Information Owner responsible for granting and revoking access to institutional information and granting and revoking permission for the use of institutional information.
7. User. User means an individual or automated application authorized to access information or information resources in accordance with the Information Owner-defined controls and access rules.
8. Separation of Duties (SOD). Separation of Duties means a security principle and control involving assigning separate tasks and responsibilities to separate individuals to reduce the risk of fraud, error, or other misconduct.

Data Classification

The UNT System Enterprise Information Security Program classifies Enterprise information into three categories:

Confidential

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. Examples include, but are not limited to, student information, social security numbers, health or medical records, and financial aid information.

Proprietary

Information not publicly available and proprietary to an institution that is controlled prior to release under the Texas Public Information Act with moderate requirements for confidentiality, integrity, or availability. Examples include, but are not limited to, grant information, donor information, patron information, and some payroll information.

Public

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 the State of Texas Public Information Act (Texas Government Code Chapter 552).

Please see the Categorization and Ownership matrix for detailed information concerning the classification of information ownership by information type and category as well as identified roles within the Enterprise with Information Owner responsibilities.

Responsibilities

Understanding Information Security

Information Security is paramount to ensure that Enterprise information is protected from unauthorized access and manipulation. Information Owners and Information Stewards must comply with the UNT System Enterprise Information Security Program including all regulations, the Information Security Handbook, policies, standards, and procedures. Failure to appropriately secure and protect Enterprise information could lead to the following:

- compromise of student, patient, or employee privacy;
- violations of FERPA, HIPAA, or other federal or State of Texas regulations;
- disruption of patient care, instructional services, and administrative functions;
- loss of reputation for the Enterprise;
- financial loss to the Enterprise resulting from payments of mandated notifications or for providing credit monitoring services to individuals whose personal data has been exposed, and payment of any regulatory fines;
- increased regulatory oversight;
- loss of good will and potential loss of donations;
- loss of grants;
- loss or corruption of research data;
- extortion, with Enterprise information being held for ransom; and
- equipment malfunctions that can impact Enterprise operations or patient care.

Ensuring Privacy and Confidentiality

Information Owners or their Information Stewards must review and approve the use of information prior to its use, processing, and storage. Information Owners may not delegate their accountability to protect Enterprise information and must ensure information under their authority is protected according to governing laws, regulations, policies, and standards set forth by the UNT System Enterprise. Governing federal and State of Texas laws include but are not limited to: the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA), Texas Administrative Code Title 1 Part 10 Chapter 202 for higher education institutions, Texas Identity Theft Enforcement and Protection Act, Texas Medical Records Privacy Act, Payment Card Industry Data Security Standards, Digital Millennium Copyright Act, the Red Flags Rule, and intellectual copyright laws.

Classifying and Inventorying Information

Information Owners are responsible for coordinating with the CISO, or their delegate, to classify all Enterprise information under their authority[1] and identify applicable privacy and security laws and the laws and regulations required to protect it.

Information Owners must keep inventories of Enterprise information under their authority and maintain records of where the information is, including its creation, processing, storage, and destruction (*See* Record Retention Schedule resources). Inventories must include a record of Enterprise information residing in both Enterprise owned or third-party information resources.

Managing Access to Information

Information Owners or their Information Stewards must grant, review, and revoke permission for the use of Enterprise information, including but not limited to: Approving requests for access, documenting individuals with access, reviewing access lists periodically, and revoking access when no longer needed or justified. Information Owners should limit access to Enterprise information based on the principle of least privilege and confirm a documented business justification.

Information Owners must maintain a list of their delegates and all individuals with access and must periodically review these records. Information Owner or their delegates should conduct reviews in accordance with the Information Security Handbook[2] and Access Control Standard[3].

Custodians called Access Control Executives (ACEs) may have the ability to retrieve information about users who can access data. Information Owners should consistently work with ACEs to ensure access information is accurate and current.

Coordinating with the Chief Information Security Officer or their Delegate

Identifying Security Controls

Information Owners must work with the CISO or their delegate to identify security controls sufficient for the protection of Enterprise information under their authority[4]. Controls must meet the requirements and standards of the UNT System Enterprise Information Security Program or relevant external elevated control requirements, such as NIST Special Publication 800-171.

[1] 1 TAC § 202.72(a)(1)(A)
[2] UNT System Information Security Handbook
[3] Access Control Standard
[4] 1 TAC § 202.72(a)(1)(D)

Security Exceptions

Information Owners should collaborate with the CISO, or their delegate, as needed for security exceptions[5]. In the event that information security controls required by the Enterprise Information Security Program cannot be met, Information Owners must work with the CISO or their delegate to determine if an exception is warranted. Information Owners are responsible for justifying, documenting, and being accountable for exceptions to security controls for Enterprise information under their authority[6].

Risk Assessments

Information Owners collaborate with the CISO or their delegate in risk assessments for Enterprise information under their authority, which includes participation in annual risk assessments of Enterprise Information Resources and additional risk assessments as needed[7]. Information Owners will assist the CISO with risk management decisions for Enterprise information under their authority.

Coordinating with Information Resource Custodians

Information Owners must also formally assign custody of Enterprise information under their authority[8]. Enterprise Custodians include but are not limited to: ACEs, UNT System Information Technology, and the UNT System Enterprise Applications team. Information Owners must ensure Custodians implement defined security controls and procedures and follow proper procedures regarding information handling and information security.

Delegation of Authority

Information Owners may delegate some responsibilities over Enterprise information; however, they may not delegate their accountability to the information under their authority. Information Stewards are responsible for all actions delegated to them by an Information Owner. Information Stewards must not further delegate their responsibilities as described in the Information Owner Delegation of Authority.

Information Owners must work with UNT System Information Technology IT Compliance to document and establish Delegations of Authority for Information Owner responsibilities to an Information Steward. Delegations of Authority must list the specific responsibilities delegated. Information Stewards must not perform responsibilities of an Information Owner for which they are not delegated.

[5] 1 TAC § 202.72(a)(1)(H)
[6] 1 TAC § 202.72(a)(1)(G)
[7] 1 TAC § 202.72(4)(A)
[8] 1 TAC § 202.72(a)(1)(C)

Information Owners may delegate the following responsibilities to an Information Steward:

- granting permission for the use of Enterprise information under their authority;
- regular review of permission granted for the use of Enterprise information under their authority;
- revoking permission for the use of Enterprise information under their authority;
- modifying or correcting Enterprise information records within Enterprise information resources;
- evaluating Separation of Duties violations within Enterprise information resources; and
- approving the establishment and use of user and service accounts within information resources with access to Enterprise information under their authority.

Information Owners <u>may not</u> delegate the following responsibilities to an Information Steward:

- coordinating with the Chief Information Security Officer (CISO) or their delegate to classify information under their authority;
- formally assigning custody of information or an information resource under their authority;
- coordinating with the CISO or their delegate to identify security controls for information systems processing information under their authority;
- conveying security control requirements to Custodians and providing them with the authority to implement;
- accountability for modifications or corrections to Enterprise information records to prevent compromise to historical Enterprise records or obfuscation of fraudulent activity;
- approving a User's direct access to database accounts within Enterprise information resources;
- approving Separation of Duties (SOD) violations or accepting risk related to SOD violations within Enterprise information systems;
- accountability and approval for security exceptions involving Enterprise information under their authority, and
- accepting risk related to the use of and access to Enterprise information under their authority.

References

- Texas Penal Code Chapter 33.02(b-1)
- Texas Administrative Code § 202.72
- Texas Administrative Code § 202.75
- UNT System Information Security Handbook

- UNT System Information Security Regulation

Document Version Log

Version	Approved By	Date	Description
1	Charlotte Russell	9/25/2017	Last documented revision
2	Charlotte Russell	4/17/2020	Added Document Version Log, added page numbers, modified naming for data classification, standard editing and review
3	Charlotte Russell	9/15/2020	Removed reference to defunct committee
4	Rich Anderson	2/16/2024	Reformatting and rewrite