Policies of the University of North Texas at Dallas	Chapter 14
14.012 Information Security Policy	**Information Technology**

Policy Statement. The University of North Texas at Dallas (UNTD) is committed to protecting the confidentiality, integrity, and availability of information and information resources. This policy supports security, business continuity, risk management, compliance with applicable laws and regulations, and maximizes the ability of the University to meet its goals and objectives.

Application of Policy. All users of information and information resources of the University, including students, faculty, staff, guests, contractors, consultants, and vendors.

Definitions.

1. Business Continuity Planning. "Business Continuity Planning" means the process of identifying mission-critical information systems and business functions, analyzing the risks and probabilities of service disruptions and outages, and developing procedures to continue operations during outages and restore those systems and functions.

2. Category I Information. "Category I Information" means confidential information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

3. Category II Information. "Category II Information" means sensitive information that could be subject to release under the Texas Public Information Act and should be controlled prior to release.

4. Category III Information. "Category III Information" means Public information available for release as described in the Texas Public Information Act.

5. Incident. "Incident" means a security event that results in, or has the potential to result in a breach of the confidentiality, integrity, or availability of information or an information resource. Security incidents result from accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or modification of information resources or information.

6. Information. "Information" means data that the University is responsible for generating, collecting, processing, accessing, disseminating, or disposing of in support of a business function.

7. Information Resources. "Information Resources" means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

8. Information Security. "Information Security" means the protection of information and information resources from threats in order to ensure business continuity, minimize business risks, and maximize the ability of the University to meet its goals and objectives. Information security ensures the confidentiality, integrity and availability of information resources and information.

9. Information Security Handbook. "Information Security Handbook" means the UNT System Information Security Handbook establishes the information security program framework for the University.

10. Information Security Program. "Information Security Program" means a collection of controls, policies, procedures, and best practices used to ensure the confidentiality, integrity, and availability of University owned information resources and information.

11. Least Privilege. "Least Privilege" means the security principle that requires application of the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

12. Mission Critical. "Mission Critical" means a function, service, or asset that is vital to the operation of UNTD which, if made unavailable, would result in considerable harm to the Institution and its ability to fulfill its responsibilities.

13. Organizational Unit. "Organizational Unit" means a department, division, center, office, or other sub-unit of UNTD. Organizational units are identified on the University organizational chart, and have staff and budget allocations.

Procedures and Responsibilities.

1. Information Security Program and Controls

UNTD is required to adopt and implement an information security program that is consistent with UNT System Regulation 06.1000. The processes, procedures, controls and standards established to meet the requirements of this policy shall adhere to the UNT System Information Security Handbook, which incorporates 1 TAC §202, the information security management system framework established in ISO/IEC 27001 and ISO/IEC 27002, NIST SP 800-53, and other information protection standards as applicable. Information protection laws shall be considered in regard to use or access to information and information resources.

Responsible Party: President, Information Security Officer, Information Owners, Custodians, Users

2. Information Security Roles

2.1. Executive Management

2.1.1 The President or his designee is responsible for overseeing the protection of information resources and for reviewing and approving the designation of information owners and their associated responsibilities.

2.1.2. The UNTD information security program shall comply with directives given by the UNT System Associate Vice Chancellor and CIO who shall be responsible for approval, oversight and coordination of the information security program throughout the UNT System.

Responsible Party: President, Information Security Officer, Information Owners, Custodians, Users

2.2. Information Security Officer

2.2.1 The Information Security Officer for the University is responsible for administration and management of the information security program and shall report to and comply with directives from the UNT System Associate Vice Chancellor and CIO.

Responsible Party: Information Security Officer

2.3. Functional Roles

2.3.1. Information owners have operational authority for specific information and are responsible for authorizing the controls for generation, collection, processing, access, dissemination and disposal of that information.

2.3.2. A custodian is the person responsible for implementing the information owner-defined controls and access to an information resource. Custodians are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by information owners for the purpose of 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 University.

2.3.3. A user is an individual or automated application authorized to access an information resource in accordance with the information owner-defined controls and access rules.

2.3.4. Guests, contractors, consultants and vendors are considered external parties and shall adhere to this policy.

Responsible Party: Information Owners, Custodians, Users, External Parties

3. Secure Access and Management of Information and Information Resources

3.1. All individuals who hold information security roles are responsible for ensuring the confidentiality, integrity, and availability of information and information resources that they access or use.

Responsible Party: Users

3.2. Access to information and information resources shall be managed and controlled and shall be granted according to the principle of least privilege.

Responsible Party: Information Owners, Custodians

3.3. Information Owners and Custodians must ensure that access to information and information resources shall be granted to a user only after the user has acknowledged that he or she will comply with this policy and shall be removed

upon termination of employment, employment status change or termination of a written agreement.

Responsible Parties: Information Owners, Custodians, Users

3.4. All users of information resources shall receive security awareness training that is based on their information security role.

Responsible Parties: Organizational Units, Users

3.5. In accordance with applicable laws, the UNT System Information Security Handbook, and this policy, information shall be classified by Information Owners as Category I, II, or III. Information Owners and Custodians shall ensure that management, use, and access to information shall be based on its classification.

Responsible Parties: Information Owners, Custodians

3.6. Information and information resources shall be protected in accordance with the controls required under the UNT System Information Security Handbook and shall be implemented to ensure their logical and physical protection during all phases of their lifecycles.

Responsible Parties: Information Owners, Custodians, Users

3.7. Risks to information resources shall be managed in accordance with the requirements of the UNT System Information Security Handbook. The expense of security safeguards shall be commensurate with the value of the information and information resources being protected.

Responsible Parties: Information Owners, Custodians, Information Security Officer, Users

4. Information Security Incident Management.

4.1. The Information Security Officer is responsible for managing security incidents.

Responsible Party: Information Security Officer

4.2. Security incidents shall be reported to the Information Security Officer and investigated promptly. All users shall cooperate during incident investigations and

shall maintain the confidentiality of incidents and associated activities during all phases of incident handling.

Responsible Parties: Information Security Officer, Information Owners, Custodians, Users

5. Business Continuity Planning. Business continuity and disaster recovery plans shall be created and maintained for mission critical information resources in accordance with the requirements of the UNT System Information Security Handbook.

   Responsible Party: Custodians

6. Security Exceptions. Exceptions to security controls may be issued by the Information Security Officer.

   Responsible Party: Information Security Officer

7. Sanctions. Penalties for violating this policy include, but are not limited to, the following: disciplinary action, access and usage loss, employment termination, criminal prosecution, civil litigation, and fines.

   Responsible Party: Information Security Officer, Users, Supervisors, and others involved in the disciplinary process

References and Cross-References.

UNT System Information Security Regulation 06.1000
UNT System Information Security Handbook
Texas Administrative Code, Title 1 §202
Texas Public Information Act
National Institute of Standards and Technology Controls (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 27000 Series, Information technology – Security techniques – Code of practice for information security management.
Payment Card Industry Data Security Standards

Approved: 7/24/17
Effective: 7/24/17
Revised: