Policy Chapter:	**Chapter 14 Information Technology**
Policy Number and Title:	**14.002 Information Security**

I. Policy Statement

The University of North Texas (UNT) 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.

II. Application of Policy

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

III. Policy Definitions

A. Business Continuity Planning

"Business Continuity Planning," in this policy, 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.

B. Confidential Information

"Confidential Information," in this policy, means 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).

C. Proprietary Information

"Proprietary Information," in this policy, means 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.

D. Public Information

"Public," in this policy, means information with low requirements for confidentiality, integrity, or availability and information intended for public release as described in the Texas Public Information Act. Public information may not be released without approval from the Office of General Counsel.

E. Custodian

"Custodian," in this policy, means a person responsible for implementing the information owner-defined controls and access to an information resource.

F. Incident

“Incident,” in this policy, 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.

G. Information

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

H. Information Resources

“Information Resources,” in this policy, means the procedures; equipment; software that are employed, designed, built, operated, maintained to collect, record, process, store, retrieve, display, and transmit information; and associated personnel including consultants and contractors.

I. Information Security

“Information Security,” in this policy, 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.

J. Information Security Program

“Information Security Program,” in this policy, means the policies, Information Security Handbook, control catalog, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions.

K. Least Privilege

“Least Privilege,” in this policy, 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.

L. Mission Critical

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

M. Organizational Unit

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

IV. Policy Responsibilities

A. Information Security Programs and Controls

UNT 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 must adhere to all applicable federal and state laws related to information resources and information security, including but not limited to 1 Tex. Admin. Code § 202 and the State of Texas Department of Information Resources Security Controls Standards Catalog (DIR Catalog). The UNT System Information Security Program is maintained by the UNT System Vice Chancellor and Chief Information Officer.

B. Information Security Roles

1. Executive Management

   The President or the president's 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. UNT Information Security Program

   The UNT Information Security Program must comply with directives given by the UNT System Vice Chancellor and Chief Information Officer who is responsible for approval, oversight, and coordination of the information security program throughout the UNT System.

3. Information Security Officer

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

4. Functional Roles

   a. Information Owners

      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.

b. Custodians

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.

c. User

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.

d. External Parties

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

C. Secure Access and Management of Information and Information Resources

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.
2. Access to information and information resources must be managed and controlled and must be granted according to the principle of least privilege.
3. Information Owners and Custodians must ensure that access to information and information resources are granted to a user only after the user has acknowledged that they will comply with this policy. Users must be removed upon termination of employment, employment status change, or termination of a written agreement.
4. All users of information resources must receive security awareness training that is based on their information security role.
5. In accordance with applicable laws, the UNT System Information Security Program, and this policy, information must be classified by Information Owners as Confidential, Proprietary, or Public. Information Owners and Custodians must ensure that management, use, and access to information is based on its classification.
6. Information and information resources must be protected in accordance with the controls required under the UNT System Information Security Program and must be implemented to ensure their logical and physical protection during all phases of their lifecycles.
7. Risks to information resources must be managed in accordance with the requirements of the UNT System Information Security Program. Security safeguards must be in direct proportion with the value of the information and information resources being protected.

D. Information Security Incident Management

The Information Security Officer is responsible for managing security incidents. Security incidents must be reported to the Information Security Officer and investigated promptly. All users must cooperate during incident investigations and must maintain the confidentiality of incidents and associated activities during all phases of incident handling.

E. Business Continuity Planning

Business continuity and disaster recovery plans must be created and maintained for mission critical information resources in accordance with the requirements of the UNT System Information Security Program.

F. Security Exceptions

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

G. 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.

V. References and Cross-References

1 Tex. Admin. Code § 202
State of Texas Department of Information Resources Security Controls Standards Catalog
Texas Public Information Act
UNT System Information Security Regulation 06.1000
UNT System Information Security Program

VI. Revision History

Policy Contact:	Director, Information Security
Approved Date:	08/01/1991
Effective Date:	08/01/1991
Revisions:	08/01/1997, 06/01/2002, 10/01/2002, 07/10/2015, 12/18/2023, 02/15/2024* *Format Only