Regulations of the University of North Texas System	Chapter 06 Information Technology
06.1000 Information Security	

06.1001 **Regulation Statement**. The University of North Texas System is committed to establishing an information security program to protect the confidentiality, integrity, and availability of information and information resources. Implementation of an information security program supports business continuity, management of risk, and maximizes the ability of the University of North Texas System, the System Administration and Institutions to meet their goals and objectives.

06.1002 **Application of Regulation**. All users of information and information resources of the System, System Administration and Institutions, including faculty, staff, students, guests, contractors, consultants, and vendors.

06.1003 **Definitions**.

1. Information Resources. 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.

2. Information Security. The protection of information and information resources from threats in order to ensure business continuity, minimize business risks, and maximize the ability of the System, System Administration and Institutions to meet their goals and objectives. Information security ensures the confidentiality, integrity and availability of information resources and information.

3. Security Handbook. The UNT System Information Security Handbook shall establish the information security program framework for the System, System Administration and Institutions. The Security Handbook shall comply with applicable federal and state laws related to information resources and information security, including but not limited to 1 Texas Administration Code §§202 and 203, as amended. The Security Handbook also shall comply with the International Standards Organization 27001 and 27002, as amended.

06.1004 Procedures and Responsibilities.

1. The UNT System Information Security Handbook.
   The System Associate Vice Chancellor for Information Technology shall be responsible for developing the Security Handbook.

   Responsible Party: Associate Vice Chancellor for Information Technology

2. Information Security Programs, Policies and Processes.
   The System Administration and Institutions are required to adopt and implement information security programs, policies and processes that are consistent with the requirements set out in the Security Handbook and shall comply with the requirements of the Security Handbook.

   Responsible Party: Information Security Officers

3. Information Security Structure.
   The following officials at the System Administration and each Institution shall comply with their assigned responsibilities as specified in this regulation and in the Security Handbook.

   a. The System or Institution Head or Designated Representative.
      The Chancellor for the System Administration and the President of each Institution or their designee is responsible for overseeing the protection of information resources and for reviewing and approving the designation of information owners and their associated responsibilities.

   b. Associate Vice Chancellor for Information Technology.
      The System Associate Vice Chancellor for Information Technology shall be responsible for approval, oversight and coordination of all information security programs for the System Administration and Institutions.

   c. Information Security Officer.
      The Associate Vice Chancellor for Information Technology or his or her designee shall appoint an Information Security Officer for the System Administration. The President of each institution or his or her designee shall appoint an Information Security Officer for the Institution. The Information Security Officer is responsible for developing and administering the operation of an information

security program. In addition to their administrative supervisors, Information Security Officers will report to and comply with directives from the Associate Vice Chancellor for Information Technology for all security related matters.

d. Information Owner.
The Information Owner is the person with operational authority for specific information and who is responsible for authorizing the controls for generation, collection, processing, access, dissemination and disposal of that information. This person shall comply with the requirements of the Security Handbook and applicable information security program.

e. Custodian.
The 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 System Administration or an Institution.

f. 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.

Responsible Party: Chancellor and Presidents or their designees, Associate Vice Chancellor for Information Technology, Information Security Officers, Information Owner, Custodian, User

4. Risk Management and Assessment.
Risks to information resources must be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected.

a. The Associate Vice Chancellor for Information Technology will commission system-wide security risk assessments of information resources as required in 1 Texas Administration Code §202.72, as amended.

b. The Associate Vice Chancellor for Information Technology and the Information Security Officers will develop risk management plans to address risks identified in the risk assessments of information resources.

c. The Chancellor for System Administration and the President of each Institution or their designee is responsible for approving the applicable risk management plan and making risk management decisions based on the risk assessment and either accept exposures or protect the data according to its value/sensitivity.

d. If a public information request for the risk management plan or a risk assessment is received, the Office of General Counsel for the System shall determine whether the requested information is exempt from disclosure under §2054.077(c) of the Texas Government Code.

Responsible Party: Associate Vice Chancellor for Information Technology, Chancellor and Presidents or their designees, Information Security Officers, Office of General Counsel

5. Biennial Review.

As required by 1 Texas Administrative Code §202.71, the information security programs for the System, System Administration and Institutions shall be reviewed biennially and revised for suitability, adequacy, and effectiveness as needed. This review shall be performed by an individual independent of the information security program. This individual shall be designated by the Associate Vice Chancellor for Information Technology and approved by the Chancellor for the System Administration and President of each Institution or their designees.

Responsible Party: Associate Vice Chancellor for Information Technology, Chancellor and Presidents or their designees

References and Cross-references.

Texas Administrative Code Title 1, Part 10, Chapter 202
Texas Administrative Code Title 1, Part 10, Chapter 203
Texas Penal Code Chapter 33
Texas Penal Code Chapter 37
International Standards Organization 27001
International Standards Organization 27002

<u>Forms and Tools</u>.
UNT System Information Security Handbook

Approved: November 19, 2013
Effective: November 19, 2013
Revised: