UNT SYSTEM

2016

Information Security Handbook

University of North Texas System
University of North Texas
University of North Texas Health Science Center
University of North Texas at Dallas

July 2016

This Page Intentionally Left Blank

Table of Contents

1. Introduction

1.1. Executive Summary

The University of North Texas System ("UNT System") Information Security Handbook establishes the information security program framework for the System Administration and Institutions. The UNT System is committed to establishing an information security program designed to protect the confidentiality, integrity, and availability of information and information resources. Implementation of an information security program supports business continuity, management of risk, enables compliance, and maximizes the ability of the System Administration and Institutions to meet their goals and objectives. The Information Security Handbook shall comply with federal and state laws related to information and information resources security, including, but not limited to the Texas Administrative Code ("TAC") Title 1 §§ 202 and 203 and the information security framework established in International Standards Organization ("ISO") 27001 and 27002.

1.2. Governance

The UNT System Information Security Handbook is governed by applicable requirements set forth in 1 TAC §§ 202 and 203 and the information security framework established in ISO 27001 and 27002. Refer to 1 TAC §§ 202 and 203 and ISO 27001 and 27002 if a topic is not addressed in the handbook or if additional guidance is needed.

1.3. Scope and Application

The requirements established in the Information Security Handbook apply to all users of information and information resources of the System Administration and Institutions, including students, faculty, staff, guests, contractors, consultants, and vendors.

1.4. Annual Review

As required by 1 TAC § 202.70, the information security program for the System Administration and Institutions shall be reviewed annually and revised for suitability, adequacy, relevance, and effectiveness as needed; this review shall be performed by a party independent of the information security program. This party 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.

2. Definitions

2.1. Access. The physical or logical capability to interact with, or otherwise make use of, information resources.

2.2. Asset. Anything of value to an organization, including information.

2.3. Breach. An incident that results in the compromise of confidentiality, integrity, or availability of information or information resources.

2.4. Business Continuity Planning. 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.

2.5. Category I Information. 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.

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

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

2.8. Confidential Information. 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).

2.9. Custodian. A 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 and Institutions.

2.10. Disaster Recovery. The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

2.11. Enterprise Information Resource. An information resource that is administered by Information Technology Shared Services ("ITSS").

2.12. Incident. 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.

2.13. Information Owner. 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.

2.14. 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.

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

2.16. Information Security Officer. The Information Security Officer is responsible for developing and administering the operation of an information security program. 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. 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.

2.17. Information Security Program. A collection of controls, policies, procedures, and best practices used to ensure the confidentiality, integrity, and availability of System Administration and Institution owned information and information resources.

2.18. Institution. A degree-granting component of the UNT System.

2.19. Integrity. The security principle that information and information resources must be protected from unauthorized changes or modifications.

2.20. Least Privilege. 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.

2.21. Mission Critical. A function, service, or asset that is vital to the operation of the Institution, which if made unavailable, would result in considerable harm to the Institution and the Institution's ability to fulfill its responsibilities.

2.22. Privileged Access. An escalated level of resource access that could allow changes to information systems potentially affecting the confidentiality, integrity, or availability of information or information resources. Privileged access is granted to users that are responsible for providing information resource administrative services such as system maintenance, data management, and user support.

2.23. Removable Media. Any device that electronically stores information and can be easily transported. Examples of removable media include USB flash drives, CD-ROM, DVD-ROM, external or portable hard drives, laptop computers, tablets, or any other portable computing device with storage capabilities.

2.24. Risk Assessment. The process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on the System Administration or an Institution's mission, functions, image, reputation, assets, or individuals. Risk assessment incorporates threat and vulnerability analysis and considers mitigations provided by planned or in-place security controls.

2.25. System Administration. The central administrative component of the UNT System.

2.26. University of North Texas System. The System Administration and the member institutions combined to form the UNT System.

2.27. User. An individual or automated application authorized to access an information resource in accordance with the Information Owner-defined controls and access rules.

3. Structure of the Information Security Handbook

The structure of the Information Security Handbook is based on the framework established in ISO 27001 and 27002. In addition, requirements of the handbook are consistent with the

Information Security Standards established in 1 TAC §§ 202 and 203, as amended.

3.1. Reference

3.1.1. UNT System Information Security Regulation 6.1000

4. Risk Management and Assessment

4.1. Purpose

Risks to information resources must be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected and the liability inherent in regulations, laws, contractual obligations, or other agreements governing the assets.

4.2. Requirements

4.2.1. The UNT System Associate Vice Chancellor for Information Technology and Chief Information Officer will commission a system-wide security risk assessment of information resources consistent with UNT System and Institutional compliance and risk assessment plans.

4.2.2. Risk assessments of mission critical and high-risk information resources shall be conducted annually. All information resources shall be assessed biennially.

4.2.3. Risk assessments must use a standard methodology that is compatible with 1 TAC § 202.75.

4.2.4. The Chancellor for System Administration and the President of each Institution or their designated representative is responsible for approving the 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 and sensitivity.

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

4.3. References

4.3.1. Texas Administrative Code, Title 1 § 202.75; Managing Security Risks

4.3.2. International Standards Organization 27002:2013; Risk Assessment and Treatment
4.3.3. International Standards Organization 27001:2013

5. Information Security Program

5.1. Purpose

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 Information Security Handbook and shall comply with the requirements of the Information Security Handbook.

5.2. Information Security Program Review

5.2.1. The Information Security Officer will conduct an annual review of the information security program to assess opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.

5.2.2. The Information Security Handbook will be reviewed and updated at least annually or as needed. The System Information Security Officer will notify campus Information Security Officers if changes are made to the Information Security Handbook.

5.2.3. A working group shall be assembled annually and as needed with representatives from the System Administration and each Institution to review and approve changes to the Information Security Handbook.

5.2.4. The System Information Security Officer will present recommendations for revision to the handbook workgroup based on the independent review and/or the System Information Security Officer review. The handbook committee can either accept or propose modifications to any recommendations. The result of the workgroup's decision should be documented and taken into account.

5.2.5. The Associate Vice Chancellor for Information Technology is responsible for approving changes made to the Information Security Handbook.

5.3. References

5.3.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head
5.3.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
5.3.3. Texas Administrative Code, Title 1 § 202.74; Institution Information Security Program
5.3.4. International Standards Organization 27002:2013; Organization of Information Security
5.3.5. International Standards Organization 27001:2013

6. Information Security Structure

6.1. Purpose

The responsibilities for managing information security are assigned to designated individuals within the organization and external to the organization. Officials of the System Administration and each Institution, as well as external entities, shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1000 and 1 TAC §§ 202.70 - 202.72 and 202.74.

6.2. Internal Organization

The following officials at the System Administration and each Institution shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1000 and 1 TAC §§ 202.70 - 202.72 and 202.74.

6.2.1. **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.

6.2.2. **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.

6.2.3. **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.

6.2.4. **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 Information Security Handbook and applicable information security program.

6.2.5. **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, but are not limited to, employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the System Administration or an Institution.

6.2.6. **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.

6.3. External Organization

6.3.1. Access, permissions, and privileges assigned to vendors, consultants, and other persons of interest must be managed and reviewed to ensure the return of all confidential and proprietary information and information

resource assets and to ensure the removal of computer access when obligations or responsibilities of an external party change.

6.3.2. Written agreements or contracts must be in place between the System Administration or Institution and external party prior to granting access to information or information resources to the external party. Security risk assessments and the use of non-disclosure agreements must also be implemented prior to entering into agreements with external parties who will access information resources, Category I, or Category II information.

6.3.3. Information resources assigned from the System Administration or Institutions to another institution of higher education, or from the System Administration or an Institution to a contractor or other third party, shall be protected in accordance with the policies, standards, and other conditions imposed by the System Administration or Institution.

6.4. References

6.4.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head
6.4.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
6.4.3. Texas Administrative Code, Title 1 § 202.72; Staff Responsibilities
6.4.4. Texas Administrative Code, Title 1 § 202.74; Institution Information Security Program
6.4.5. International Standards Organization 27002:2013; Organization of Information Security
6.4.6. International Standards Organization 27001:2013

7. Asset Management

7.1. Purpose

The System Administration and Institutions must maintain a documented inventory of institutionally-owned physical assets associated with information processing. Information and information resources must also be identified, classified, documented, and have documented owners. Policies and procedures must be developed to ensure the security of information resource assets against unauthorized or accidental modification, destruction, or disclosure. These controls are to ensure the confidentiality, integrity, and availability of information and other assigned information resources.

7.2. Responsibility for Information Assets

The System Administration and Institutions shall identify the owner of information resources along with their responsibilities, to include Information Owners, Custodians and users of information resources. They shall define and document the responsibilities for the information resources.

7.3. Information Classification and Handling

7.3.1. Categories of Information

Information must be classified. The following information classification system shall be used to categorize information for risk assessments, making risk management decisions, establishing controls, and for protecting information:

7.3.1.1. Category I includes 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, and judicial requirements), legal agreements, or information that requires a high degree of confidentiality, integrity, or availability. Category I information must be labeled and protected.

7.3.1.2. Category II includes information that is proprietary to an institution or has moderate requirements for confidentiality, integrity, or availability.

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

7.3.2. The System Administration and Institutions must prohibit the storage of Category I data on personally owned devices without appropriate security controls.

7.3.3. The System Administration and Institutions must manage access to information based on its classification.

7.3.4. The System Administration and Institutions must comply with the Department of Information Resources ("DIR") Security Controls Standards Catalog, as required by 1 TAC § 202.76.

7.3.5. The institution of higher education head or his or her designated representative(s) shall review and approve Information Ownership and associated responsibilities to include personnel, equipment, or information technology hardware and software.

7.4. Information Safeguards

7.4.1. Controls must be implemented to provide physical, technical, and procedural safeguards for information resources by the Custodians of information resources that include external parties providing outsourced information resources services.

7.4.2. The System Administration and Institutions must dispose of electronic records and devices according to the DIR Security Controls Standards Catalog, and as required by 1 TAC § 202.76.

7.4.3. Category I information shall be labeled as confidential in physical and electronic formats except in cases where the asset is encrypted.

7.4.4. The principle of Least Privilege must be established and enforced when developing standards**,** procedures, or assigning access permissions.

7.5. References

7.5.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head
7.5.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
7.5.3. Texas Administrative Code, Title 1 § 202.72; Staff Responsibilities
7.5.4. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
7.5.5. International Standards Organization 27002:2013; Asset Management
7.5.6. International Standards Organization 27001:2013

8. Human Resources Security

8.1. Purpose

All employees and contractors must understand their roles and responsibilities pertaining to information security. Employee and contractor access to information and information resources must be reviewed and modified when employment status changes occur and due to termination or changes in written agreements.

8.2. Prior to Employment

The System Administration and Institutions must ensure that employees receive information security awareness training and must inform new employees about security policies and procedures prior to granting access to information resources.

8.3. During Employment

Supervisors must require that employees complete annual information security awareness training. Employees shall be provided training for handling sensitive data as appropriate for the employee's role.

8.4. Termination or Changes of Employment

The System Administration and Institutions must have exit procedures in place to ensure the return of all confidential and proprietary information and information resource assets upon termination of employment or written agreement and ensure the timely removal of computer access when the employment status, contractual obligation, or responsibilities of an individual changes.

8.4.1. Responsibilities and duties that change or remain valid after termination should be contained in a written agreement or contract between the employee and the System Administration or Institution.

8.4.2. The terminating employee's immediate supervisor is responsible for managing security aspects of the termination, including the return of assets, the removal of access rights, and providing notification to information owners of the change in access**.**

8.4.3. Changes of responsibilities of employment should be managed by previous and new supervisors as roles are terminated and new roles initiated.

8.5. References

8.5.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
8.5.2. International Standards Organization 27002:2013; Human Resources Security
8.5.3. International Standards Organization 27001:2013
8.5.4. Payment Card Industry Data Security Standards 3.0

9. Physical Security

9.1. Purpose

Implementation of physical security measures help to protect information and information resources from unauthorized access. Physical security is a critical aspect of information security.

9.2. Secure Areas

9.2.1. The System Administration and Institutions must document and manage physical security for mission critical information resources to ensure confidentiality, integrity, and availability of information resources.

9.2.2. All information processing facilities must be protected by physical controls that are appropriate for the size and complexity of the operations and the criticality, sensitivity, regulatory compliance requirements, and risks to the systems or services operated at those locations.

9.2.3. Work areas must be protected in accordance with physical controls and security requirements that are appropriate for the type of operational functions performed in the area. The System Administration and Institutions shall develop procedures to distinguish between onsite personnel and visitors in sensitive areas.

9.2.4. Physical security and emergency procedures for information resources must be documented, tested, and reviewed as part of the risk assessment process.

9.2.5. On-site personnel shall only be granted access to information processing facilities in accordance with job responsibilities.

9.2.6. Personnel should be made aware of the existence of, or activities within, a secure area on an as-needed basis.

9.2.7. Personnel working in secure areas must be supervised. The level of supervision should be appropriate for the type of operational function performed in the area, adhere to the relevant regulatory compliance requirements, and consider identified applicable risks.

9.2.8. Secure areas should be locked, or otherwise secured, and periodically inspected.

9.2.9. The use of equipment to photograph, record video, and/or record audio is prohibited in secure areas unless explicitly authorized by the administrator of the secure area.

9.3. Equipment Security

9.3.1. Procedures for protecting mission critical information resources from environmental hazards, power failures, and other disruptions must be documented, updated, and tested at least annually.

9.3.2. Employees shall be designated to train and monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

9.3.3. Office areas and computer screens should remain clear of Category I information when a device or office is unattended.

9.3.4. Category I information should never be left unattended on media such as printers, fax machines, and other devices.

9.3.5. Category I information in print or stored on media should be locked away when not required for use or when an office is vacant. Physical media includes, but is not limited to computers, removable storage devices, and printed information.

9.3.6. Unattended computers and terminals should be logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar authentication mechanism.

9.3.7. Use of photocopiers, scanners, digital cameras, and other reproduction technology for unauthorized duplication of Category I data is prohibited.

9.4. Equipment Maintenance

Equipment must be maintained in accordance with the supplier's recommended service intervals and specifications.

9.4.1.1. Only authorized maintenance personnel should carry out repairs or service equipment.

9.4.1.2. Records should be kept of all preventative and corrective equipment maintenance.

9.4.1.3. Records should be kept of all suspected or actual equipment errors.

9.4.1.4. Controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel onsite or external to the organization. Where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared.

9.4.1.5. Vendor or service provider maintenance recommendations must be followed.

9.4.1.6. Equipment must be inspected and tested prior to placing in operation to ensure integrity and proper function.

9.5. References

9.5.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
9.5.2. International Standards Organization 27002:2013; Physical and Environmental Security
9.5.3. International Standards Organization 27001:2013

10. Communications and Operations Management

10.1. Purpose

Documented operating procedures must be implemented to protect data communications, minimize interruption to business activities, and ensure the integrity and availability of information.

10.2. Operational Procedures and Responsibilities

10.2.1. The principle of Least Privilege must be established and enforced when developing standards, procedures, or assigning access permissions.

10.2.2. A separation of functions must be established for tasks involving information and information resources that are susceptible to fraudulent or other unauthorized activity.

10.2.3. The System Administration and Institutions must follow password policies and procedures, established by the System Administration or Institution, that provide the password management service and are also consistent

with ISO 27002 and the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

10.2.4. The System Administration and Institutions must follow policies and procedures that govern access, management, and monitoring of communication networks and devices that are established by the System Administration or Institution providing communications service consistent with ISO 27002 and the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

10.2.5. The System Administration and Institutions must implement controls to protect information and information resources from malicious or unauthorized code. The System Administration or Institution providing the service is responsible for establishing standards for management of anti-virus protection.

10.2.6. The System Administration and Institutions must create procedures for the use of digital signatures that comply with provisions found in 1 TAC § 203.

10.3. System Planning and Acceptance

10.3.1. The System Administration and Institutions shall establish policies and procedures ensuring that security reviews take place prior to contracting with external parties. The reviews must meet the requirements of the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76, which includes signing of a non-disclosure agreement if confidential data will be used as part of the agreement.

10.3.2. As part of the annual risk assessment process, the System Administration and Institutions shall require reviews of contracted third party services to ensure continued compliance with agreed upon security and compliance standards.

10.4. Protection Against Malware, Malicious, or Unwanted Programs

The System Administration and Institutions shall establish policies and procedures regarding malware, malicious, or unwanted programs. Policies and procedures should address malware on system, application, and network layers.

10.4.1. Centrally administered antivirus software must be installed on all information resources managed by System Administration or Institutions.

10.4.2. Antivirus software must be kept current.

10.4.3. Antivirus software must be configured so that users cannot disable or prevent the software from functioning properly.

10.4.4. Information resources must be scanned on a periodic basis for malware, malicious, or unwanted programs.

10.5. Back-Up

The System Administration and Institutions are required to regularly backup and test mission critical information. Backup processes shall be defined to protect the confidentially, integrity, and availability of the stored information.

10.6. Network Security Management

The System Administration and Institutions should develop policies and procedures for the secure management, access, monitoring, and control of institutionally owned and managed communications networks. Policies or procedures should require the following:

10.6.1. Access to the network must be restricted to authorized devices and users. Network access must be logged or otherwise documented;

10.6.2. Network access must adhere to the principle of Least Privilege;

10.6.3. Secure remote access procedures must be developed and communicated;

10.6.4. Networks must be segmented by function;

10.6.5. Appropriate security controls must be implemented based on the criticality and value of the resources on the network;

10.6.6. Networks must be monitored; and

10.6.7. Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided internally or outsourced.

10.7. Media Handling

The System Administration and Institutions must implement policies and procedures regarding the secure management of removable media. Policies should address

encryption, storage, transport, and the secure destruction of any data commensurate with the value and sensitivity of the information.

10.7.1. Any physical media containing Category I information must be protected in accordance with the requirement set by the Information Owner and any laws, regulations or standards governing the information. Physical media includes, but is not limited to computers, removable storage devices, and printed information.

10.7.2. Strict protection controls over media containing Category I information must be maintained by the Custodian of the media. The chain of custody must be tracked if the media is transported beyond its original location and transferred to another Custodian.

10.7.3. Protections should include using reliable couriers that are bonded and insured, maintaining chain of custody by keeping accurate logs of the content of the media, the protection applied, times of transfer to the alternate location, receipt at the destination and appropriately protecting media during transit.

10.8. Exchange of Information

10.8.1. The System Administration and Institutions must implement policies and procedures ensuring that the exchange of information within and external to the organization is secure.

10.8.2. Information exchanged with an external institution, agency, or organization must be protected as required by the System Administration or Institution policies in accordance with the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

10.8.3. The transfer of information to an external institution, agency, or organization must be governed by information transfer agreements to ensure the confidentiality and integrity of institutionally owned data. Information transfer agreements should include the following:

10.8.3.1. Management responsibilities for controlling and notifying transmission dispatch and receipt;

10.8.3.2. Procedures to ensure traceability and non-repudiation;

10.8.3.3. Minimum technical standards for packaging and transmission;

10.8.3.4. Escrow agreements;

10.8.3.5. Courier identification standards;

10.8.3.6. Responsibilities and liabilities in the event of information security incidents, such as loss of data;

10.8.3.7. Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

10.8.3.8. Technical standards for recording and reading information and software;

10.8.3.9. Any special controls that are required to protect sensitive items, such as cryptography;

10.8.3.10. Maintaining a chain of custody for information while in transit; and

10.8.3.11. Acceptable levels of access control.

10.9. Electronic Commerce

Electronic commerce security protections shall be defined where applicable to ensure the protection of online transactions. The Payment Card Industry Data Security Standards ("PCI DSS") must be followed for any institution accepting payment card transactions as appropriate. Third-party processors must also demonstrate compliance with PCI DSS.

10.10. Monitoring

10.10.1. Monitoring and logging processes shall be established that provide a sufficiently complete history of transactions for auditing purposes and that meet the requirement of the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76.

10.10.1.1. Monitoring and logging functions must provide audit trails to ensure accountability for updates to mission critical information, hardware, and software.

10.10.1.2. Event logs that record user activities, exceptions, faults, and information security events should be produced, maintained, and regularly reviewed for enterprise systems.

10.10.2. Controls must be established to ensure the confidentiality and integrity of information in system logs, transaction histories, and other system audit information. Access to this information must be monitored and stored in a location that is separate from the systems generating the information.

10.10.3. The System Administration and Institutions must implement system identification/logon banners, which have warning statements that indicate the system is the property of the System Administration or an Institution. The identification/logon banner shall include the following topics at minimum:

10.10.3.1. Unauthorized use is prohibited;

10.10.3.2. Usage may be subject to security testing and monitoring;

10.10.3.3. Misuse is subject to penalties and/or criminal prosecution; and

10.10.3.4. Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

10.11. References

10.11.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
10.11.2. Texas Administrative Code, Title 1, Chapter 203; Management of Electronic Transactions and Signed Records
10.11.3. International Standards Organization 27002:2013; Communications and Operations Management
10.11.4. International Standards Organization 27001:2013
10.11.5. UNT System Password Standards

11. Access Control

11.1. Purpose

Care should be taken to ensure that no single person can access, modify, or use assets without authorization or detections.

11.1.1. Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of assets.

11.2. User Access Management

11.2.1. The System Administration and Institutions shall ensure user access is managed by establishing procedures for granting accounts, managing passwords, regular review of accounts and associated privileges, and reviewing accounts immediately upon change of employment status. Privileges must be limited to the needs of individual users.

11.2.2. User behavior, activities, or the use of computing devices to access institutional networks must not compromise the security of users, information, or information resources.

11.2.3. Institutional or external networks must not be used to compromise the identity of or impersonate individuals or information resources.

11.2.4. Privileged access to information resources shall be only be granted as required by business need or job duties.

11.2.5. Privileged access will be granted in accordance with the principle of Least Privilege.

11.2.6. Privileged access will be granted and maintained in accordance with the UNT System Information Ownership Guide.

11.2.7. Privileged access to information resources will not be granted unless explicitly authorized by the Information Owners or their delegates.

11.2.8. The duration of privileged access shall not last longer than needed to perform functional job duties.

11.2.9. Privileged access rights will be assigned to a different user ID than those used for regular day-to-day activities.

11.2.10. Users with privileged access rights must have the appropriate skills and knowledge to maintain the confidentiality, integrity, and availability of the information resources for which they are granted access. Users with privileged access rights must certify their skills and knowledge to maintain privileged access.

11.2.11. The use of default privileged accounts should be avoided. If it is necessary to use accounts of this nature, compensating controls must be employed to ensure the security of the information resources.

11.2.12. The immediate supervisor of an employee, whose employment status changes, shall notify the Information Owners about the change as soon as possible.

11.2.13. Information Owners must review access rights in accordance with the UNT System Information Ownership Guide.

11.3. User Responsibilities

11.3.1. Users are responsible for all activities related to their accounts.

11.3.2. Users must keep their accounts and passwords secure.

11.3.2.1. Passwords must not be shared with anyone and are considered Category I information.

11.3.2.2. Passwords must be protected during automatic log on sessions.

11.3.2.3. Users must adhere to the UNT System Password Standards.

11.3.3. Users should only access information and use information resources that are required to perform job duties.

11.4. Operating System Access Control

The System Administration and Institutions shall develop policies and procedures that govern access to operating systems of institutionally owned computing devices and servers.

11.4.1. Access to operating systems should be controlled by a secure log on procedure.

11.4.2. All users should have a unique identifier which should be used to trace activities to the responsible individual.

11.4.3. Log on banners specifying a user's rights and responsibilities regarding system usage should be presented to users during the log on process.

11.4.4. Administrator access should be limited to those individuals who have a documented business reason for the access.

11.4.5. Users may not employ tools or utilities capable of overriding system and application controls without permission.

11.4.6. Administrator accounts or accounts with expanded privileges should only be used for administration and management of information resources.

11.4.7. Shared administrator accounts or accounts with expanded privileges will only be granted based on a documented business need. Controls must be implemented to mitigate the risk arising from the use of shared administrator accounts or accounts with expanded privileges.

11.4.7.1. The identity of a user must be verified prior to the activation of an administrator account or an account with expanded privileges.

11.4.7.2. Users authorized for shared administrator accounts or accounts with expanded privileges must agree to keep authentication information confidential and maintained solely within the group authorized to use the privileged account. Authentication information must change if group membership changes.

11.4.7.3. Default vendor authentication information must be changed following installation of systems or software.

11.4.8. Users with administrator accounts or accounts with expanded privileges must adhere to the System Administrator Code of Ethics as referenced in 11.8.4.

11.4.9. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in the UNT System Password Standards.

11.4.10. Authorizations for privileged access rights must be reviewed at regular intervals. Changes to privileged accounts must be documented.

11.4.11. Inactive sessions should be terminated after a defined period of inactivity.

11.5. Application and Information Access Control

11.5.1. Access to applications and application data should be restricted according to the principle of Least Privilege.

11.5.2. Users may not employ tools or utilities capable of overriding application controls.

11.5.3. Access to mission critical applications and Category I application data should be logged or documented by other means.

11.5.4. Shared administrator accounts or accounts with expanded privileges will only be granted based on a documented business need. Controls must be implemented to mitigate the risk arising from the use of shared administrator accounts or accounts with expanded privileges.

11.5.5. The identity of a user must be verified prior to the activation of an administrator account or an account with expanded privileges.

11.5.6. Users authorized for shared administrator accounts or accounts with expanded privileges must agree to keep authentication information confidential and maintained solely within the group authorized to use the privileged account. Authentication information must change if group membership changes.

11.5.7. Default vendor authentication information must be changed following installation of systems or software.

11.5.8. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in the UNT System Password Standards.

11.5.9. Authorizations for privileged access rights must be reviewed at regular intervals. Changes to privileged accounts must be documented.

11.5.10. Inactive sessions should be terminated after a defined period of inactivity.

11.6. Mobile Computing and Teleworking

11.6.1. Users must follow security policies and procedures when accessing institutional resources and information remotely.

11.7. References

11.7.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
11.7.2. International Standards Organization 27002:2013; Access Control
11.7.3. International Standards Organization 27001:2013
11.7.4. System Administrator Code of Ethics
11.7.5. UNT System Password Standards
11.7.6. UNT System Information Ownership Guide

12. Information Systems Acquisition, Development, Testing, and Maintenance

12.1. Purpose

Security requirements should be identified and included in development, acquisition, testing, maintenance, and implementation of information resources.

12.2. Security Requirements of Information Systems

12.2.1. Security and compliance requirements must be considered in all phases of computer system or software development lifecycles and the systems acquisition process.

12.2.2. The System Administration and Institutions must implement change or configuration management processes for controlling modifications to hardware, software, firmware, and documentation.

12.2.3. The requirements of the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76, must be implemented when testing data or managing test, development, and quality assurance environments.

12.2.4. The System Administration and Institutions must implement policies and procedures to manage operating system and software updates and patches that follow industry best practice or provide compensating controls to mitigate risk resulting from out of date software.

12.3. Correct Processing in Applications

12.3.1. The System Administration and institutions must develop and implement procedures to ensure the confidentiality, integrity, and availability of information if the institution engages in software engineering or development.

12.4. Cryptographic Controls

12.4.1. The System Administration and Institutions must develop policies and procedures implementing encryption requirements for information storage devices, data transmission, portable devices, removable media, and encryption key standards based upon the requirements established by the Institution providing the service. Minimum encryption requirements must include the following:

12.4.1.1. Confidential information transmitted over a public network must be encrypted;

12.4.1.2. Confidential information stored in a public location that is directly accessible without compensating controls in place must be encrypted;

12.4.1.3. Storing confidential information on portable devices should be discouraged;

12.4.1.4. Confidential information must be encrypted if copied to or stored on a portable computing device, removable media, or non-agency owned computing device;

12.4.1.5. In instances where no technology exists to encrypt a device, compensating electronic controls must be implemented to secure the device;

12.4.1.6. Encryption of a device must be documented and verifiable; and

12.4.1.7. Encryption keys must be managed.

12.4.2. The System Administration and Institutions must encrypt institutionally-owned mobile devices. If a device is not capable of encryption, no Category I data may be stored on the device.

12.5. Security in Development and Support Processes

Information security must be considered in all phases of the system development lifecycle or acquisition process.

12.5.1. The System Administration and Institutions should establish standards for the secure development of software, systems, and architecture; and should also consider the following:

12.5.1.1. Security of the development environment;

12.5.1.2. Security in the software development methodology;

12.5.1.3. Secure coding guidelines for each programming language used;

12.5.1.4. Security requirements in the design phase;

12.5.1.5. Security checkpoints within the project milestones;

12.5.1.6. Secure repositories;

12.5.1.7. Security in version control;

12.5.1.8. Required application security knowledge; and

12.5.1.9. Developers' capability of avoiding, finding, and remediating vulnerabilities.

12.5.2. System administrators are responsible for maintaining the security of systems and keeping software up to date.

12.5.3. Systems that are no longer supported by the vendor will not be allowed to connect to the institution network without compensating controls approved by the office of the Information Security Officer.

12.5.4. Development, testing, and operational environments should be separate for all systems to reduce the risks of unauthorized access or changes to the operational environment.

12.6. Technical Vulnerability Management

12.6.1. The System Administration and Institutions must implement policies and procedures for vulnerability assessment and management.

12.6.1.1. Only documented and authorized individuals may perform vulnerability assessments.

12.6.1.2. Institutions must create policy and procedures for vulnerability management that include acceptable time frames for addressing vulnerabilities and escalation procedures for handling unaddressed vulnerabilities.

12.7. References

12.7.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
12.7.2. International Standards Organization 27002:3; Information Systems Acquisition, Development, Testing, and Maintenance
12.7.3. International Standards Organization 27001:2013

13. Supplier Relationships

13.1. Purpose

System Administration and Institutions must establish procedures to manage supplier and vendor access to information and information resources.

13.2. Information Security in Supplier Relationships

Procedures to manage supplier and vendor access to information and information resources must include:

13.2.1. Identification of the types of suppliers and vendors who may have access to institutionally owned information and information resources;

13.2.2. Standardized processes and lifecycle management for supplier and vendor relationships;

13.2.3. Processes for monitoring and controlling the access to information and information resources;

13.2.4. Security awareness training and awareness for personnel involved in acquisitions regarding applicable policies, processes and procedures; and

13.2.5. Awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behavior based on the type of supplier and the level of supplier access to the organization's systems and information.

13.3. Documentation Requirements for Initiating Supplier Relationships

Explicit documentation of information security requirements must be established for information and information resources used by suppliers and vendors prior to the initiation of the relationship. Documentation should include:

13.3.1. Explicit documentation of the access to information and information resources that will be granted to suppliers and vendors for a particular engagement;

13.3.2. Processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

13.3.3. Controls established to ensure the integrity of the information or information processing provided by either party;

13.3.4. Incident handling procedures and contingencies associated with supplier or vendor access including responsibilities of both the organization and suppliers;

13.3.5. Controls established to ensure the availability of the information or information processing provided by either party;

13.3.6. Conditions under which information security requirements and controls will be documented in an agreement signed by both parties; and

13.3.7. Procedures for managing the transition of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

13.4. Supplier Service Delivery Management

System Administration and Institutions shall regularly monitor, review and audit supplier service delivery and agreements. A service management relationship process should exist with the supplier and should address the following:

13.4.1. Monitor service performance levels to verify adherence to the agreements;

13.4.2. Review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

13.4.3. Conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

13.4.4. Provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

13.4.5. Review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

13.4.6. Resolve and manage any identified problems;

13.4.7. Review information security aspects of the supplier's relationships with their suppliers; and

13.4.8. Ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

13.5. Changes to Supplier Services

System Administration and Institutions shall document the process for managing changes to supplier services, including the following:

13.5.1. Changes to Supplier Agreements.

13.5.2. Changes made by the organization for implementing:

13.5.2.1. Enhancements to the current services offered;

13.5.2.2. Development of any new applications or systems;

13.5.2.3. Modifications or updates of the organization's policies and procedures; and

13.5.2.4. New or changed controls to resolve information security incidents and to improve security.

13.5.3. Changes in supplier services for implementing:

13.5.3.1. Changes and enhancements to networks;

13.5.3.2. Use of new technologies;

13.5.3.3. Adoption of new products or newer versions/releases;

13.5.3.4. New development in tools and environments;

13.5.3.5. Changes to physical location of service facilities;

13.5.3.6. Change of suppliers; and,

13.5.3.7. Sub-contracting to another supplier.

13.6. References

13.6.1. International Standards Organization 27002:2013; Supplier Relationships
13.6.2. International Standards Organization 27001:2013

14. Information Security Incident Management

14.1. Purpose

Incident response procedures are necessary to ensure all staff understand their responsibilities for reporting incidents as well as to promote timely and thorough responses to incidents.

14.2. Reporting Information Security Events and Weaknesses

14.2.1. The System Administration and Institutions must establish information security incident management procedures that consider all phases of incident handling.

14.2.2. Information security breaches must be investigated promptly and reported to the Information Security Officer.

14.3. Management of Information Security Incidents and Improvements

14.3.1. In accordance with the requirements set forth in the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76, the Information Security Officer will assess the incident, oversee incident response, assemble incident response teams as necessary, and will coordinate incident handling, remediation, and reporting. Custodians and Information Owners must cooperate with incident investigations.

14.3.2. As required by 1 TAC § 202.73 information security breaches must be reported to the DIR if they propagate to other state systems, result in criminal violations that are required to be reported to law enforcement, or

involve the unauthorized disclosure or modification of confidential information.

14.3.3. Confidentiality of incidents and associated activities must be maintained during all phases of incident handling.

14.4. References

14.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
14.4.2. Texas Administrative Code, Title 1 § 202.73; Security Reporting
14.4.3. International Standards Organization 27002:2013; Information Security Incident Management
14.4.4. International Standards Organization 27001:2013

15. Business Continuity Management

15.1. Purpose

The System Administration and Institutions shall develop and maintain business continuity and disaster recovery plans for mission critical information resources. They shall also develop alternative procedures that enable personnel to continue critical day-to-day operations in the event of the loss of information resources.

15.2. Development of Business Continuity and Disaster Recovery Plans

15.2.1. Business continuity and disaster recovery plans must include a business impact analysis, risk assessment, and a disaster recovery plan as required by the DIR Security Controls Standards Catalog, as required by 1 TAC § 202.76. The business impact analysis determines which information resources are critical.

15.2.2. Business continuity and disaster recovery plans must consider information security, should be tested at least annually, and shall be updated as frequently as needed.

15.3. Annual testing of redundant and high-availability information resources is required to ensure failover configurations work as intended.

15.4. The System Associate Vice Chancellor for Information Technology must review and approve the business continuity plan for mission critical enterprise information resources. ISO 22301 is to be used for the framework for all business continuity plans to ensure consistency as required by ISO 27001.

15.5. The Information Security Officers for the System Administration and Institutions shall distribute business continuity and disaster recovery plans for information resources to key personnel and store a copy offsite.

15.6. References

15.6.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
15.6.2. International Standards Organization 27002:2013; Business Continuity Management
15.6.3. International Standards Organization 27001:2013
15.6.4. International Standards Organization 22301:2013; Societal Security -- Business Continuity Management Systems -- Requirements

16. Compliance with Legal Requirements

16.1. Purpose

The System Administration and Institutions are required to identify and adhere to all legal, regulatory, contractual requirements, UNT System Regulations, System Administration Policies, and Institutional Policies.

16.2. Data Protection Laws

Information protection laws and standards must be considered in regard to use or access to information and information resources. Laws and standards include, but are not limited to, the following: Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA), Texas Identity Theft Enforcement and Protection Act, Texas Medical Records Privacy Act, Payment Card Industry Data Security Standards, Digital Millennium Copyright Act, and intellectual copyright laws.

16.2.1. Information Owners and their delegates are responsible for identifying, documenting, and keeping up to date with all relevant legislative, statutory, regulatory, and contractual requirements relative to the information in their control. Custodians are responsible for implementing information security controls based on information protection laws and standards identified by owners

16.3. Acknowledgement of Security Responsibilities

All users of information and information resources of the System Administration and

Institutions, including faculty, staff, students, guests, contractors, consultants, and vendors shall acknowledge and abide by the security controls governed by relevant legislative, statutory, regulatory, and contractual requirements.

16.4. Information Systems Audit Considerations

Information Owners, Custodians, and their delegates should ensure information systems and audit control activities involving verification of operational systems should be regularly planned and agreed to minimize risks and disruptions to business processes. The following guidelines should be observed during information systems audits:

16.4.1. Audit requirements for access to systems and data should be agreed upon with appropriate management.

16.4.2. The scope of technical audit tests should be agreed upon and controlled.

16.4.3. Audit tests should be limited to read-only access to software and data.

16.4.4. Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.

16.4.5. Requirements for special or additional processing should be identified and agreed upon.

16.4.6. Audit tests that could affect system availability should be run outside business hours.

16.4.7. All access should be monitored and logged, where appropriate, to produce a reference trail

16.5. References

16.5.1. International Standards Organization 27002:2013; Compliance with Legal Requirements
16.5.2. International Standards Organization 27001:2013

17. Security Exceptions

The System Administration and Institutions shall implement procedures for granting and documenting security exceptions in accordance with 1 TAC §§ 202.71, 202.72, and 202.73.

The Information Security Officer, with the approval of the institution of higher education head or his or her designated representative, may issue exceptions to information security requirements or controls. The Information Security Officer will coordinate exceptions and compensating controls with information and service owners. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

18. Sanctions for Violations

Penalties for violating the requirements of this handbook include but are not limited to disciplinary action, loss of access and usage, termination, prosecution, and/or civil action.

Appendix A
System Administrator Code of Ethics

1. Introduction

Certain designated persons are given broader access to the resources of information resources because their job responsibilities require such access. Typically, such persons are responsible for providing administrative services on the designated information resources such as system maintenance, data management, and user support. The term "broader access" covers a range -from wider access than given to an ordinary system user, up to and including complete access to all information resources. Persons with the broadest (complete) access are sometimes called "superusers."

2. Application

This code of ethics applies to all persons given broader-than-normal access to any information resources. It also applies to persons who authorize such access. The points contained in this code are considered additions to the responsibilities acknowledged by all ordinary information resources users and by the authorizers of information resources privileges.

3. Responsibilities of Privileged Access Users

Superusers (individuals with full access to files) and all other persons given broader-than-normal access privilege to information resources agree:

3.1. Not to "browse" through information while using the powers of privileged access unless such browsing: is a specific part of their job description (e.g., an auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious, system-impairing behavior, and/or possible violations of policy; is specifically requested by, or has the approval of, the person who authorized their privileged access. Browsing should never be done unless it is in the best interest of the institution.

3.2. Not to disclose, to any unauthorized person, information observed while operating with privileged access.

3.3. Not to copy any information for any purpose other than those authorized under their defined job responsibilities or pursuant to an authorized investigation or review.

3.4. Not to intentionally or recklessly damage or destroy any information or information resource.

3.5. Not to accept favors or gifts from any user or other person potentially interested in gaining access to information or information resources.

3.6. Not to do any special favors for any user, member of management, friend, or any other person regarding access to information or information resource. Such a favor would be anything that circumvents prevailing security protections or standards.

3.7. Not to disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.

3.8. Not to attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.

3.9. Not to change or develop any information resources software in a way that would disclose information to persons not authorized to have it, or make it possible to retain any special access privilege once that authorized privilege has been terminated by management.

3.10. Not to make arrangements on information resources under their charge that will impair the security of other information resources. In order to comply with this restriction, a system administrator setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.

Furthermore, superusers and all other persons given broader-than-normal access privileges on information resources agree that they will:

3.11. Report all suspicious requests, incidents, and situations regarding an information resource to the Information Security Officer and to institutional law enforcement.

3.12. Use all available software protections to safeguard information resources under their charge from unauthorized access by any person or other information resources.

3.13. Take steps to the best of their ability to comply with all information security standards and policies in force and furthermore, advise management and/or designated information security representatives of deficiencies in these standards.

3.14. Conduct themselves in a manner that will foster security awareness and understanding among users.

Appendix B
Handbook References

1. Regulations

a. Texas Administrative Code, Title 1, Section 202

2. Industry Guidelines

a. International Standards Organization 27001:2013
b. International Standards Organization 27001:2013

3. System Administration Policies, Regulations, and Publications

a. UNT System Regulation 06.1000 Information Security
b. UNT System Password Standards
c. UNT System Information Ownership Guide

4. Handbook Contributors

Name	Title	Entity
Rama Dhuwaraha	Chief Information Officer and Associate Vice Chancellor for Information Technology	UNT System Administration University of North Texas University of North Texas at Dallas
Charlotte Russell	Chief Information Security Officer	UNT System Administration University of North Texas University of North Texas at Dallas
Richard Anderson	Information Technology Security Director	UNT System Administration University of North Texas University of North Texas at Dallas
Pamela Johnson	Assistant Director, Management and Risk Services	UNT System Administration University of North Texas University of North Texas at Dallas
Paula Mears	Information Technology Security Analyst Lead	UNT System Administration University of North Texas University of North Texas at Dallas
Christine Sikes	Information Technology Compliance Analyst	UNT System Administration University of North Texas University of North Texas at Dallas

Katy Gallahan	Information Technology Support Director, Campus Technology Support Services	UNT System Administration
Philip Baczewski	Senior Director, University Information Technology	University of North Texas
Michael Hollis	Senior Systems Analyst, Product Development and Engineering	University of North Texas Health Science Center
Nathan Ribelin	Director, Help Desk and Client Services	University of North Texas Health Science Center
Kevin Rocha	IT Support Manager, Campus Technology Support Services	University of North Texas at Dallas UNT System Administration

Appendix C
Document Version Log

Version	Approved By	Date	Description
1	Charlotte Russell	06/04/2014	
2	Charlotte Russell		Updated Texas Administrative Code References
3		05/15/2016	Incorporated Third-Party Recommendations
4		05/31/2016	Formatted for Presentation to the Security Handbook Working Group
5		06/17/2016	Information Security Handbook Working Group Initial Review changes
6	Charlotte Russell	06/27/2016	Information Security Handbook Working Group Final Review Changes
7	Rama Dhuwaraha	07/13/2016	Chief Information Officer Revisions