UNT SYSTEM

2020

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

_____2020

This Page Intentionally Left Blank

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 Information Security Handbook contains procedures and standards that support adherence to UNT System Information Security Regulation 6.100. 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 and Chief Information Officer and approved by the Chancellor for the System Administration and President of each Institution or their designees.

2. Information Security Definitions

2.1. Definitions

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

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

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

2.1.4. 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.

2.1.5. Category I Confidential 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.

2.1.6. Category II Proprietary Information. Information that is proprietary to an Institution or has moderate requirements for confidentiality, integrity, or availability.

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

2.1.8. Change Management. The process responsible for controlling the life-cycle of changes made to information resources that are implemented while maintaining the confidentiality, integrity and availability of the information resource.

2.1.9. 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).

2.1.10. Configuration Management. A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

2.1.11. Custodian. A person responsible for implementing the Information Owner-defined controls and access to information and 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.

2.1.12. 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.

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

2.1.14. High Impact Information Resource. An Information Resource whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

2.1.14.1. Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

2.1.14.2. Result in major damage to organizational assets;

2.1.14.3. Result in major financial loss; or

2.1.14.4. Result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

2.1.15. 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, disruption, or modification of information or information resources.

2.1.16. 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.

2.1.17. Information Resources. The procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information and associated personnel including consultants and contractors.

2.1.18. 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 and information resources.

2.1.19. Information Security Officer. The Information Security Officer is responsible for developing and administering the operation of an information security program. The Associate Vice Chancellor and Chief Information Officer, 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 and Chief Information Officer for all security related matters.

2.1.20. 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.

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

2.1.22. Integrity. The security principle that information and information resources must be protected from unauthorized change or modification.

2.1.23. 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.

2.1.24. Mission Critical. A function, service, or asset 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.

2.1.25. Network Devices. Hardware components or software services running on common desktop or information resources that communicate over the institution's network.

2.1.26. Patch. An update to an operating system, application, or other software issued to correct specific problems.

2.1.27. Patch Management. The systematic notification, identification, deployment, installation, and verification of operating system and application software patches.

2.1.28. Penetration Test. A series of activities undertaken to identify and exploit security vulnerabilities.

2.1.29. Personally Identifying Information. Information that alone or in conjunction with other information identifies an individual, including an individual's:

2.1.29.1. Name, social security number, date of birth, or government-issued identification number;

2.1.29.2. Mother's maiden name;

2.1.29.3. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

2.1.29.4. Unique electronic identification number, address, or routing code; and

2.1.29.5. Telecommunication access device as defined by Section 32.51, Penal Code.

2.1.30. Privileged Access. An escalated level of resource access that allows changes to information systems and could affect 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.

2.1.31. Recovery Point Objective (RPO). The maximum tolerable period in which data might be lost from an IT service due to a major incident. (i.e., amount of potential data loss).

2.1.32. Recovery Time Objective (RTO). The duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

2.1.33. 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.

2.1.34. Residual Risk. The risk that remains after security controls have been applied.

2.1.35. Risk. The effect on the mission, function, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact.

2.1.36. 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.

2.1.37. Security Exception. An exception granted by the Chief Information Security Officer in response to non-compliance resulting from an inability to meet the requirements of an information security policy, standard, or procedure.

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

2.1.39. Transaction Risk Assessment. An evaluation of the security and privacy requirements for an interactive web session providing public access to an institution’s information and services.

2.1.40. University of North Texas System. The System Administration and the member Institutions combined to form the UNT System.

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

2.1.42. Vulnerability Assessment. A documented evaluation assessing the extent to which an information resource or data processing conducted by the UNT System Administration or Institutions or by a third-party is vulnerable to unauthorized access or harm, is subject to attack, and the extent to which electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

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. Failure to respond to risks could result in accidental or intentional acceptance of institutional risk by an unauthorized individual.

4.2. Requirements

4.2.1. The UNT System Associate Vice Chancellor and Chief Information Officer will commission a system-wide security risk assessment of information resources consistent with UNT System Administration 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. The risk assessment process must consider the immediate and future impact of a risk to organizational operations.

4.2.4. Risk assessments must use a standard methodology compatible with 1 TAC § 202.75. Identified risks shall be accepted, rejected, mitigated, or transferred using a defined and documented plan.

4.2.5. 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.

4.2.6. The Chancellor or President is authorized to make risk management decisions for residual high risks.

4.2.7. The Information Security Officer is authorized to make risk management decisions for residual moderate and low risks.

4.2.8. 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. Reference

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
4.3.4. National Institute of Standards and Technology 800-30; Guide for Conducting Risk Assessments.

5. Information Security Program

5.1. Purpose

The System Administration and Institutions are required to adopt and implement information security programs, policies, and processes 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 and Chief Information Officer is responsible for approving changes made to the Information Security Handbook.

5.3. Reference

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. Organizational Structure of Information Security

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 and Chief Information Officer

The System Associate Vice Chancellor and Chief Information Officer 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 and Chief Information Officer 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 Confidential, or Category II Proprietary 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. Reference

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. Human Resource Security

7.1. Purpose

The System Administration and Institutions must establish rules that describe the responsibilities and expected behaviors of all users of institutional information systems. These rules shall be updated regularly according to security and institutional policy changes. 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.

7.2. Access Agreements

Employee and contractor access to institutional information and information resources shall be preceded by access agreements.

7.2.1. Access agreements shall include a signed acknowledgment that the user understands responsibilities and expected behaviors of accessing institutional information resources.

7.2.2. Access agreements must be reviewed, modified, and acknowledged as changes are made to user responsibilities and expected behaviors.

7.2.3. Access agreements must be reviewed, modified, and acknowledged in the event of employment status changes, terminations, or changes in written agreements.

7.3. Prior to Employment

7.3.1. The System Administration and Institutions must ensure that employees receive certified cybersecurity/information security awareness training and must inform employees about security policies and procedures during the onboarding process and prior to granting access to information resources.

7.3.2. Employees of the System Administration and Institutions with direct responsibilities concerning institutional information resources must complete information security/cybersecurity training directly proportional to their responsibilities and job duties, including but not limited to continuing education.

7.4. During Employment

7.4.1. Employees must complete annual certified cybersecurity/information security awareness training. Employees shall be provided training for handling sensitive data as appropriate for the employee's role.

7.4.2. Supervisors must document and monitor employee security training and retain employee training records for one year or until superseded by subsequent training and must be prepared to respond to internal reviews to confirm compliance.

7.5. 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.

7.5.1. 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.

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

7.5.3. Changes of responsibilities of employment should be managed by an employee's former and new supervisors as roles are terminated and new roles initiated. Former supervisors should review roles, privileges, and physical access to ensure that access no longer needed is disabled. New supervisors should review roles, privileges, and physical access to ensure that access needed for new job responsibilities is granted in accordance with Least Privilege and as appropriate for the sensitivity of the position.

7.6. Reference

7.6.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
7.6.2. International Standards Organization 27002:2013; Human Resources Security
7.6.3. International Standards Organization 27001:2013
7.6.4. Payment Card Industry Data Security Standards 3.0

8. Asset Management

8.1. Purpose

The System Administration and Institutions must maintain a documented inventory of institutionally-owned physical assets associated with information processing. Information and information resource assets must be identified, classified, documented, prioritized according to criticality, have documented owners, have documented custodians, and be managed through the system development life cycle. 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.

8.2. Responsibility for Information and Information Resource Assets

8.2.1. The System Administration and Institutions shall identify owners, custodians, and users of information and information resource assets and document their responsibilities.

8.2.2. Information Owners must maintain inventories of vendors or third parties that access or process institutional information.

8.2.3. Custodians and Information Owners must conduct and maintain inventories of information resources that collect, use, maintain, and/or share confidential information or Personally Identifying Information.

8.2.4. Custodians that manage, use, and/or store confidential information must develop an inventory of data that documents data flow mapping, how data are transmitted, and storage locations of confidential data.

8.2.5. Custodians of information resources that manage, use, and/or store confidential information must maintain inventories of critical information system components.

8.3. Information Classification and Handling

8.3.1. Categories of Information

Information must be inventoried and 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:

8.3.1.1. 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 confidential information must be labeled and protected.

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

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

8.3.2. Information Owners are responsible for identifying information, supporting inventories of information, and classifying information under their authority with the established information security classification categories.

8.3.3. Custodians are responsible for conducting inventories of information systems and technology for which they manage, administer, or for which they have been assigned custody.

8.3.4. The Information Security Officer is responsible for reviewing the institution's inventory of information systems and related ownership and security responsibilities.

8.4. Information Safeguards

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

8.4.2. The System Administration and Institutions must dispose of electronic records and devices according to institutional record retention policies and by employing sanitization methods with the strength and integrity in proportion to the security classification and confidentiality of information.

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

8.4.4. New computer applications and services that receive, maintain, and/or share confidential data must be reviewed to ensure compliance with data security requirements.

8.4.5. Security requirements must be identified and risk mitigation plans must be developed, contractually agreed upon, and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data.

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

8.4.7. Information systems accessible to the public should not contain Category I confidential or Category II proprietary information.

8.4.8. Information posted to publicly accessible systems should be reviewed prior to posting and at least annually to ensure neither Category I confidential or Category II proprietary information is included.

8.4.9. Users may view Category III public information on public websites or other publicly available information systems without authentication or identification.

8.5. Reference

8.5.1. Texas Administrative Code, Title 1 § 202.70; Responsibilities of the Institution Head
8.5.2. Texas Administrative Code, Title 1 § 202.71; Responsibilities of Information Security Officer
8.5.3. Texas Administrative Code, Title 1 § 202.72; Staff Responsibilities
8.5.4. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
8.5.5. International Standards Organization 27002:2013; Asset Management
8.5.6. International Standards Organization 27001:2013

9. Access Control

9.1. Purpose

The System Administration and Institutions shall establish policies and procedures to ensure that no single person can access, modify, or use assets without authorization or detection.

9.2. User Access Management

9.2.1. The System Administration and Institutions shall ensure user access is managed with established procedures related to account creation, monitoring, control, and removal, including but not limited to: Authorization, approval for access by data owners, acknowledgment of user responsibilities, managing passwords, periodic access reviews, and prompt removal of access during role change or termination.

9.2.2. User access to information and information resources shall be restricted according to the principle of Least Privilege.

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

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

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

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

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

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

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

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

9.2.11. 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.

9.2.12. 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.

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

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

9.3. **Password Standards**

Passwords are a critical control used to control access and protect the confidentiality, integrity, and availability of institutionally owned information and information resources.

9.3.1. Passwords must meet or exceed the following standards for all systems owned or managed by UNT System and Component Institutions:

9.3.1.1. Passwords must have a minimum length of 8 characters;

9.3.1.2. Passwords have a maximum length of 30 characters;

9.3.1.3. Password complexity must include uppercase letters, lowercase letters, and digits;

9.3.1.4. Spaces and backslash are prohibited characters; and

9.3.1.5. The use of common dictionary words is prohibited.

9.3.2. Credentials used for UNT System or Institution owned information resources must not be reused on other systems or services.

9.3.3. Users must change passwords at least annually. The password expiration period may be shorter for some systems based on business or compliance needs.

9.3.4. The use of shared or generic privileged accounts, such as Administrator or root, should be avoided if possible. These accounts should only be used for maintenance, system repair, or recovery operations. They should not be used for day to day operation.

9.3.4.1. The credentials for any system or generic account should be changed from the default value supplied by the vendor before the system is placed in a production capacity or is put on a public network.

9.3.4.2. Credentials for generic privileged accounts for system critical to business operations must be escrowed with the system administrator's supervisor and backup personnel.

9.3.4.3. Passwords for shared or generic privileged accounts must be changed when any employee with access to the credentials leaves the organization or changes roles within the organization. This should be done before the employment change occurs if possible to ensure the confidentiality, integrity, and availability of the information resource tied to the credentials.

9.3.5. Administrative and privileged account password composition and complexity that does not meet these requirements must have mitigating controls approved by the UNT System Chief Information Security Officer.

9.3.6. The UNT System Chief Information Security Officer may grant an exception if a system is unable to accommodate these requirements.

9.4. **User Responsibilities**

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

9.4.2. Users must keep their accounts and passwords secure.

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

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

9.4.5. Users must adhere to Section 9.3, Password Standards.

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

9.5. **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.

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

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

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

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

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

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

9.5.7. 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.

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

9.5.9. 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.

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

9.5.11. Users with administrator accounts or accounts with expanded privileges must adhere to the System Administrator Code of Ethics as referenced in Appendix A of this document.

9.5.12. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in Section 9.3, Password Standards.

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

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

9.5.15. User accounts will be locked upon 10 sequential failed login attempts and remain locked for at least 15 minutes. Privileged access accounts should remain locked until reset by an administrator.

9.6. Application Access Control

9.6.1. Use of applications is restricted to use terms as described in contract agreements.

9.6.2. Applications protected by quantity licenses should be tracked to control unauthorized copying and distribution.

9.6.3. Use of peer-to-peer file sharing technology must be controlled and documented to prevent unauthorized distribution or reproduction of copyrighted work.

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

9.6.5. Access to mission critical applications should be logged or documented by other means.

9.6.6. 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.

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

9.6.8. 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.

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

9.6.10. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in Section 9.3, Password Standards.

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

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

9.6.13. User accounts will be locked upon 10 sequential failed login attempts and remain locked for at least 15 minutes. Privileged access accounts or accounts for mission critical applications should remain locked until reset by an administrator.

9.6.14. Access through internal connections should be authorized by resource type and documented according to the interface characteristics, security requirements, and information classification.

9.7. Information Access Control

9.7.1. Access to data should be restricted according to the principle of Least Privilege.

9.7.2. Access to Category I confidential information should be logged or documented by other means.

9.7.3. Access to information through internal connections should be authorized by resource type and documented according to the interface characteristics, security requirements, and information classification.

9.8. Mobile Computing and Teleworking

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

9.9. Reference

9.9.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
9.9.2. International Standards Organization 27002:2013; Access Control
9.9.3. International Standards Organization 27001:2013

9.9.4. System Administrator Code of Ethics
9.9.5. UNT System Information Ownership Guide

10. Cryptographic Controls

10.1. Purpose

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.

10.2. Requirements

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

10.2.2. Minimum encryption requirements must include the following:

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

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

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

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

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

10.2.2.6. Encryption of a device must be documented and verifiable.

10.2.2.7. Encryption keys must be managed.

11. Physical and Environmental Security

11.1. 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.

11.2. Secure Areas

11.2.1. 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; including maintaining records concerning the entrance and exit times of onsite visitors. Records concerning access to secure areas should be maintained in accordance with institutional retention policies.

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

11.2.3. Work areas must be protected in accordance with physical controls and security requirements 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.

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

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

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

11.2.7. 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.

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

11.2.9. 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.

11.3. Equipment Security

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

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

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

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

11.3.5. Category I confidential 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.

11.3.6. 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.

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

11.4. Equipment Maintenance

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

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

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

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

11.4.5. 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.

11.4.6. Vendor or service provider maintenance recommendations should be followed pending the existence of operational or risk management considerations. Compensating controls or security exceptions must exist if vendor or service provider maintenance recommendations cannot be followed.

11.4.7. Equipment must be inspected and tested prior to placing in operation to ensure integrity and proper function and to verify that all potentially impacted security controls are intact.

11.4.8. Maintenance activities must be monitored and approved with explicit approval required for removal of equipment.

11.5. **Reference**

11.5.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
11.5.2. International Standards Organization 27002:2013; Physical and Environmental Security
11.5.3. International Standards Organization 27001:2013

12. Operations Security

12.1. **Purpose**

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

12.2. **Operational Procedures and Responsibilities**

12.2.1. The System Administration and Institutions of critical services and critical systems must develop and annually update a security plan for tht service.

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

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

12.2.4. 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.

12.2.5. 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.

12.2.6. 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.

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

12.2.8. 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:

12.2.8.1. Unauthorized use is prohibited;

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

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

12.2.8.4. Users have no expectation of privacy except as otherwise

provided by applicable privacy laws.

12.2.8.5. By using or accessing a university information resource you consent to allowing the institution to collect identifiable information that includes unique electronic identification numbers, routing codes, network address, internet protocol address, and other information that is collected from your browser, device, or information that is provided by you during your use of the information resource.

12.3. System Planning and Acceptance

12.3.1. 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 or shared as part of the agreement.

12.3.2. 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.

12.4. 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.

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

12.4.2. Antivirus software must be kept current.

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

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

12.4.5. Personal computing information resources owned by the System Administration and its Institutions must meet the following standards:

12.4.5.1. Communicate with the security management server every 120 days;

12.4.5.2. Have antivirus definitions installed that are no more than seven days old; and

12.4.5.3. Run supported versions of the antivirus software, security management server, and antivirus engine.

12.4.6. IT Managers are responsible for providing the following support to computing devices:

12.4.6.1. Installing current versions of antivirus and encryption software on all newly acquired laptops prior to deployment;

12.4.6.2. Ensuring laptop computers receive updates and patches;

12.4.6.3. Investigating laptop computers that do not meet the standards established in 12.4.3. of this standard and documenting any variances from compliance;

12.4.6.4. Resolving variances from compliance that fall within their support responsibilities; and

12.4.6.5. Removing laptop computers from security management server when decommissioned or no longer in use.

12.4.7. If variances to compliance cannot be resolved, the custodial department must submit a request for a security exception. Security exception requests must be submitted to the UNT System Office of Chief Information Security Officer and include the following:

12.4.7.1. The custodial department name, location, and contact.

12.4.7.2. The service and asset tag numbers of the laptop computer.

12.4.7.3. Location of the laptop computer.

12.4.7.4. Current use of the laptop computer.

12.4.7.5. Reason why the variance cannot be resolved.

12.4.7.6. Reason why the laptop computer cannot be decommissioned.

12.4.7.7. Compensating controls that may mitigate the risk of non-compliance.

12.4.7.8. Supplemental documentation that may exist in support of the request.

12.5. 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.

12.6. 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.

12.6.1. Any physical media containing Category I confidential information must be protected in accordance with the requirements set in the Information Security Handbook, by the Information Owner, and as required in applicable laws, regulations or standards governing the information. Copying of data should be based on user access rights and authorizations approved by the Information Owner.

12.6.2. Strict protection controls over media containing Category I confidential 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.

12.6.3. 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.

12.7. **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.

12.8. **Monitoring**

12.8.1. Custodians must establish security monitoring and logging practices. Monitoring activities should include procedures for contacting Information Security to report activities that indicate a security incident has occurred. Logs should be retained in accordance with operational and compliance needs and should include histories of transactions that capture system and user authentication, and must comply with the requirements of the DIR Security Controls Standards Catalog, as required by 1 TAC 202.76.

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

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

12.8.2. 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.

12.8.3. The organization must retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

12.9. **Internet Website and Mobile Applications**

12.9.1. The developer of a website or mobile application that processes confidential information must submit to IT Compliance the following information:

12.9.1.1. a description of the website or application architecture

12.9.1.2. the authentication mechanism for the website or application

12.9.1.3. administrator-level access to data included in the website or application

12.9.1.4. a security plan to establish planned beta testing for the website or mobile application biannually

12.9.2. The developer or entity acquiring a website or mobile application that processes sensitive personal or personally identifiable information or confidential information must subject the website and mobile application to vulnerability and penetration testing and address any vulnerability identified in the test before deployment or acquisition.

12.10. **Reference**

12.10.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

12.10.2. Texas Administrative Code, Title 1, Chapter 203; Management of Electronic Transactions and Signed Records

12.10.3. International Standards Organization 27002:2013; Communications and Operations Management

12.10.4. International Standards Organization 27001:2013

13. Communications Security

13.1. **Purpose**

The System Administrations and Institutions must develop policies and procedures to protect institutional data, minimize interruption to business activities, and ensure the integrity and availability of information.

13.2. **Network Security Management**

13.2.1. 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:

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

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

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

13.2.1.4. Networks must be segmented by function;

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

13.2.1.6. Networks must be monitored; and

13.2.1.7. 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.

13.2.2. Network Connections

13.2.2.1. Only authorized network devices may connect to University networks. The introduction of network devices or information resources that negatively affect the behavior or security of the network or violate University policies, are prohibited.

13.2.2.2. The addition of network devices that could conflict with other approved devices on the network, alter the institution's network topology, or place high demands on network bandwidth must be approved by the Chief Technology Officer prior to their introduction. The following examples of types of devices require approval:

13.2.2.2.1. Multicasting;

13.2.2.2.2. Services that answer broadcast messages, such as DHCP and BOOTP;

13.2.2.2.3. Devices that answer ARP requests as servers (such as security tools and network management tools);

13.2.2.2.4. Firewalls that operate at a level higher than a single machine in the network hierarchy;

13.2.2.2.5. Routers;

13.2.2.2.6. Bridges;

13.2.2.2.7. Switches;

13.2.2.2.8. Proxy servers;

13.2.2.2.9. Wireless access points;

13.2.2.2.10. High bandwidth devices; and

13.2.2.2.11. Other similar devices.

13.2.2.3. If a device on the network is found to compromise any aspect of the network's operation, IT Shared Services in coordination with the local IT support, may remove the device from the network.

13.3. **Information Transfer**

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

13.3.2. 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.

13.3.3. Controls should be established to ensure confidential information leaving UNT System is protected with encryption.

13.3.4. 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:

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

13.3.4.2. Procedures to ensure traceability and non-repudiation;

13.3.4.3. Minimum technical standards for packaging and transmission;

13.3.4.4. Escrow agreements;

13.3.4.5. Courier identification standards;

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

13.3.4.7. 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;

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

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

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

13.3.4.11. Acceptable levels of access control.

13.4. **Reference**

13.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

13.4.2. Texas Administrative Code, Title 1, Chapter 203; Management of Electronic Transactions and Signed Records

13.4.3. International Standards Organization 27002:2013; Communications and Operations Management

13.4.4. International Standards Organization 27001:2013

14. Information System Acquisition, Development, Testing, and Maintenance

14.1. Purpose

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

14.2. Security Requirements of Information Systems

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

14.2.2. The System Administration and Institutions must implement change and configuration management processes for controlling modifications to hardware, software, firmware, and documentation. Custodians must document and implement baseline configurations for all network devices and information systems. Changes to baseline configurations must be reviewed and approved through established change control and configuration management procedures to ensure compliance.

14.2.3. Custodians must implement change management procedures that include security impact analysis, testing and communication to affected users prior to deployment of changes. Change management must be considered in project management practices.

14.2.4. 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.

14.2.5. Information resources must be designed and configured to protect Personally Identifying Information and confidential data.

14.2.6. Multi-user information systems must be reviewed for security compliance by the Information Security Officer or designee prior to placing into production and before configuration or other changes occur.

14.2.7. Custodians of information resources must manage information resources in a manner that ensures that updates and patch management practices ensure compliance with vendor's recommended update and patch intervals, as indicated in best practice, or provide comparable compensating controls that mitigate risk resulting from out-of-date software. Patch management implementation must include:

14.2.7.1. Prioritization of patches and system updates;

14.2.7.2. Specification that patches are to be applied at regular intervals;

14.2.7.3. Aligned maintenance windows with vendor patch and update release schedules;

14.2.7.4. Patch monitoring for correct installation;

14.2.7.5. Problems shall be addressed as they occur; and

14.2.7.6. Contingency plans for handling emergency or critical updates.

14.2.8. The System Administration and Institutions must protect documents or guidelines of information systems from unauthorized disclosure that include:

14.2.8.1. Secure configuration, installation, and standard operating procedures;

14.2.8.2. Effective use and maintenance of security functions;

14.2.8.3. Known vulnerabilities regarding configuration and use of administrative functions;

14.2.9. The System Administration and Institutions must implement policies and procedures to develop continuous monitoring of information system security controls.

14.3. **Correct Processing in Applications**

14.3.1. 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.

14.4. **Security in Development and Support Processes**

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

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

14.4.1.1. Security of the development environment;

14.4.1.2. Security in the software development methodology;

14.4.1.3. Secure coding guidelines for each programming language used;

14.4.1.4. Security requirements in the design phase;

14.4.1.5. Security checkpoints within the project milestones;

14.4.1.6. Secure repositories;

14.4.1.7. Security in version control;

14.4.1.8. Required application security knowledge; and

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

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

14.4.3. Custodians are responsible for developing security plans for information resources that they manage. Security plans should include consideration of networks, facilities, systems, and other information resources.

14.4.4. Applications and information systems must be designed to align with the enterprise architecture framework. Security requirements must be included in base architecture during information technology development, acquisition and deployment.

14.4.5. 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.

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

14.5. **Vulnerability Management**

14.5.1. The System Administration and Institutions must implement policies and procedures for vulnerability assessment and management as failure to meet these conditions could result in accidental or intentional acceptance of institutional risk by an unauthorized individual.

14.5.1.1. Vulnerability assessment and system patching will only be performed by designated individuals.

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

14.5.1.3. Vulnerability scanning tools will be used to perform scans of information technology systems to identify information security vulnerabilities.

14.5.1.4. Vulnerabilities will be identified through active monitoring and reviewing of third-party vulnerability sources for any old, new or unique vulnerabilities that currently exist.

14.5.1.5. The information security officer or designee is the only official authorized to perform, approve, and initiate vulnerability assessments or penetration tests.

14.5.1.6. Penetration tests will be conducted by an authorized individual or validated third party to identify which vulnerabilities can be exploited by threat actors.

14.5.1.7. Each vulnerability alert and patch release must be checked against existing systems and services prior to taking any action to avoid unnecessary remediation.

14.5.1.8. Information Security and Custodians shall evaluate and assign urgency for each vulnerability based on the intrinsic qualities of the vulnerability, the criticality of the business systems that it affects, and the sensitivity of the data that can be found on the specific assets.

14.5.1.9. Custodians are responsible for remediating vulnerabilities identified during the vulnerability assessment process and through any other methodologies that reveal security weaknesses.

14.5.1.10. Custodians must remediate identified vulnerabilities within acceptable timeframes in order to prevent proliferation or escalation, and to prevent increases in risks to information and information resources. Vulnerabilities rated high risk must be addressed immediately.

14.5.1.11. The remediation options will be identified based on numerous risk factors including the availability of a patch and the risk accepted by utilizing a different method.

14.5.1.12. If remediation is not implemented custodians will:

14.5.1.12.1. Implement compensating controls;

14.5.1.12.2. Follow the risk management process; or

14.5.1.12.3. Pursue an exception.

14.5.1.13. All configuration and inventory documentation must be immediately updated to reflect applied remediation.

14.5.1.14. Vulnerability management will be considered as new systems and assets are deployed.

14.5.1.15. Before deploying a website or mobile application, the System Administration and Institutions must ensure language is included in third-party contracts that require the System Administration or Institution or an agreed-upon third-party to conduct vulnerability and penetration tests of the website or mobile application.

14.5.1.16. In lieu of facilitating a vulnerability or penetration test prior to deploying a website or mobile application, third-parties may provide evidence to the Information Security Officer that testing of the current configuration of the website or mobile application has occurred that complies the UNT System Information Security Handbook and application federal and state laws for protecting information resources and data security.

14.5.1.17. The System Administration and Institutions must inform third parties of the intention to conduct vulnerability and penetration tests in advance.

14.5.1.18. The System Administration and Institutions must obtain confirmation from third parties that they understand the requirement for conducting the vulnerability and penetration test and approve the actions in advance of deployment.

14.6. **Information System Maintenance**

14.6.1. The System Administration and Institutions must maintain a list of maintenance organizations and institutional personnel who are authorized to perform maintenance on multi-user information systems and develop procedures to ensure that:

14.6.1.1. Personnel performing maintenance on multi-user information systems have required access authorizations.

14.6.1.2. Designated personnel with required access authorizations and technical competence will supervise the maintenance activities of personnel who do not possess the required access authorizations.

14.6.2. Custodians are responsible for ensuring that preventative and routine maintenance is performed in a timely manner on information resources. Maintenance of information resources must be scheduled and documented.

14.6.3. Remote maintenance and diagnostic connections must be documented and approved in advance.

14.6.4. Strong authentication must be used to establish remote maintenance and diagnostic connections.

14.6.5. Remote access and diagnostic connection shall be terminated upon completion of remote system maintenance.

14.6.6. Remote maintenance and diagnostic activities must be consistent with the other security policies in the handbook.

14.7. Reference

14.7.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

14.7.2. International Standards Organization 27002:3; Information Systems Acquisition, Development, Testing, and Maintenance

14.7.3. International Standards Organization 27001:2013

15. Vendor Relationships

15.1. Purpose

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

15.2. Information Security in Vendor Relationships

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

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

15.2.2. Standardized processes and lifecycle management for vendor relationships;

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

15.2.4. Cybersecuirty/information security awareness training at the beginning of contract terms as well as any renewal with completion tracked IT Security;

15.2.5. Awareness for personnel involved in acquisitions regarding applicable policies, processes, and procedures; and

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

15.3. Documentation Requirements for Initiating Vendor Relationships

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

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

15.3.2. Language in vendor contracts concerning cybersecurity/information security awareness training;

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

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

15.3.5. Incident handling procedures and contingencies associated with vendor access including responsibilities of both the organization and vendors;

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

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

15.3.8. 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.

15.4. **Vendor Service Delivery Management**

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

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

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

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

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

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

15.4.6. Resolve and manage any identified problems;

15.4.7. Review information security aspects of the vendor's relationships with their vendors; and

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

15.5. **Changes to Vendor Services**

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

15.5.1. Changes to Vendor Agreements.

15.5.2. Changes made by the organization for implementing:

15.5.2.1. Enhancements to the current services offered;

15.5.2.2. Development of any new applications or systems;

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

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

15.5.3. Changes in vendor services for implementing:

15.5.3.1. Changes and enhancements to networks;

15.5.3.2. Use of new technologies;

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

15.5.3.4. New development in tools and environments;

15.5.3.5. Changes to physical location of service facilities;

15.5.3.6. Change of vendors; and,

15.5.3.7. Sub-contracting to another vendor.

15.6. **Reference**

15.6.1. International Standards Organization 27002:2013; Supplier Relationships
15.6.2. International Standards Organization 27001:2013

16. Information Security Incident Management

16.1. **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.

16.2. **Reporting Information Security Events and Weaknesses**

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

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

16.3. Management of Information Security Incidents and Improvements

16.3.1. 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, reporting, and the authorization of forensic analysis as necessary. Custodians and Information Owners must cooperate with incident investigations.

16.3.2. Supervisors shall provide employees training for handling sensitive data and responding to incidents as appropriate for the employee's role.

16.3.3. An incident response resource reporting to the Information Security Officer, shall assist and advise information system users in the handling and reporting of security incidents.

16.3.4. Automated mechanisms shall be employed to increase the availability of incident response-related information and support.

16.3.5. 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.

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

16.4. Reference

16.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

16.4.2. Texas Administrative Code, Title 1 § 202.73; Security Reporting

16.4.3. International Standards Organization 27002:2013; Information Security Incident Management

16.4.4. International Standards Organization 27001:2013

17. Business Continuity Management

17.1. 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.

17.2. Development of Business Continuity and Disaster Recovery Plans

17.2.1. 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 and should reflect information resource priorities based on the criticality of the resource, recovery time objectives, and recovery point objectives for data.

17.3. Requirements

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

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

17.3.3. The System Associate Vice Chancellor and Chief Information Officer 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.

17.3.4. 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.

17.3.5. The System Administration and Institutions must train employees in their contingency roles and responsibilities with respect to the information system and provide periodic refresher training as necessary.

17.4. **Reference**

17.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog
17.4.2. International Standards Organization 27002:2013; Business Continuity Management
17.4.3. International Standards Organization 27001:2013
17.4.4. International Standards Organization 22301:2013; Societal Security -- Business Continuity Management Systems – Requirements

18. Compliance with Legal Requirements

18.1. **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.

18.2. **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.

18.2.1. 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

18.3. **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.

18.4. 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:

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

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

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

18.4.4. 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.

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

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

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

18.5. Reference

18.5.1. International Standards Organization 27002:2013; Compliance with Legal Requirements

18.5.2. International Standards Organization 27001:2013

19. Privacy

19.1. Purpose

All users of information assets must protect the privacy of information assets according to governing laws, regulations, policies, and standards adopted and set forth by the UNT System and its component Institutions, including but not limited to: FERPA, HIPAA, and the Red Flags Rule.

19.2. **Responsibilities**

19.2.1. The UNT System Administration and Institutions must limit the collection, use, processing, and disclosure of Personally Identifying Information to that which serves to meet its function and purpose.

19.2.2. The use of Personally Identifying Information should be restricted to the purpose for which it was collected.

19.2.3. Personally Identifying Information should be accurate and a reasonable effort exhibited to keep the information up to date.

19.2.4. Personally Identifying Information should be kept no longer than necessary for the purpose of processing as it was originally collected.

19.2.5. Personally Identifying Information should be processed and protected with security controls proportional to the information's confidentiality.

19.2.6. Information owner consent is required prior to processing special kinds of Personally Identifying Information; including but not limited to: Genetic information, biometric information and health information.

19.2.7. Custodians shall not process Personally Identifying Information except under permissions granted by the Information Owner.

19.2.8. Employees, contractors, and other third-parties must complete privacy awareness training prior to receiving access to institutional information assets.

19.3. **Privacy and Institutional Websites**

19.3.1. The System Administration and Institutions must post the following on websites that process Personally Identifying Information: The types of data collected when visiting the website; how collected information is used; how collected information is protected; and whether collected information is shared.

19.3.2. A transaction risk assessment must be conducted prior to providing access to information or services on a website that requires Personally Identifying Information. Privacy and security safeguards must be implemented on websites that transmit, collect or store Personally Identifying Information.

19.3.3. Website key entry points must include links to the institution's Privacy policy.

19.3.4. Websites must include the following text: "By using or accessing a university website you consent to allowing the institution to collect identifiable information that includes unique electronic identification numbers, routing codes, network address, internet protocol address, and other information that is collected from your browser, device, or information that is provided by you during your use of the website."

19.3.5. The System Administration and Institutions must create and publish a privacy notice on all key public entry points or site policy pages that describes applicable provisions of the institutional privacy policy. The notice must meet all requirements of 1 TAC § 206.72.

19.4. **Reference**

19.4.1. Texas Administrative Code, Title 1 § 202.76; Security Controls Standards Catalog

20. General Security Exceptions

20.1. **Purpose**

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. The UNT System Office of the Chief Information Security Officer will provide an approval or rejection of a request for security exception to the custodial department. The UNT System Office of the Chief Information Security Officer may revoke security exceptions at any time.

21. 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, as determined by UNT System Administration and Institutions.

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

1.1. Texas Administrative Code, Title 1, Section 202

2. Industry Guidelines

2.1. International Standards Organization 27001:2013
2.2. **International Standards Organization 27002:2013**

3. System Administration Policies, Regulations, and Publications

3.1. UNT System Regulation 06.1000 Information Security
3.2. UNT System Information Ownership Guide

4. Handbook Contributors

Name	Title	Entity
Chris McCoy	Chief Information Officer	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 of Information Technology Compliance and Planning 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
Brandi Webster	Information Technology Compliance Analyst	UNT System Administration University of North Texas University of North Texas at Dallas

Name	Title	Entity
Patrick Lampkin	Information Technology Support	UNT System Administration
Philip Baczewski	Executive Director, University Information Technology	University of North Texas
Michael Hollis	Information Security Officer	University of North Texas Health Science Center
Patrick Holler	Information Technology Support, Campus Technology Support Services	University of North Texas at Dallas

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	Charlotte Russell	06/27/2016	Information Security Handbook Working Group Final Review Changes
4	Rama Dhuwaraha	07/13/2016	Chief Information Officer Revisions
5	Charlotte Russell	11/06/2017	Information Security Handbook Working Group Final Review Changes
6	Charlotte Russell	6/3/2019	Information Security Handbook Working Group Final Review Changes
7		8/31/2020	Information Security Handbook Working Group