UNT SYSTEM™
Information Technology

2023 UNT System Information Security Handbook

Table of Contents

Introduction

a. 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 6.1000. 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 Gramm-Leach Bliley Act (GLBA), Texas Government Code Chapter 2054, Texas Administrative Code ("TAC") Title 1 § 202, the Texas Cybersecurity Framework, and the Texas Department of Information Resources Information Security Standards Catalog (DIR Catalog).

b. Governance

The UNT System Information Security Handbook is governed by applicable requirements set forth in Texas Government Code Chapter 2054, 1 TAC § 202, the Texas Cybersecurity Framework, and the DIR Catalog. Refer to 1 TAC § 202, the Texas Cybersecurity Framework, and the DIR Catalog if a topic is not addressed in this Handbook or if additional guidance is needed.

c. Scope and Application

The requirements established in the Information Security Handbook apply to all members of the UNT System community with access to information and information resources of the UNT System. See Roles and RACI for further information about defined roles and responsibilities.

d. Program Review

The Vice Chancellor and Chief Information Officer (VC/CIO) shall commission an annual review of the UNT System Information Security Program which the Associate Vice Chancellor and Chief Information Security Officer (CISO) shall coordinate. The annual Information Security Program review shall assess the program's suitability, adequacy, relevance, and effectiveness. In accordance with 1 TAC §202.70, the Chancellor of the System Administration or their designee shall annually review and

approve the UNT System Information Security Program. Every other year, a party independent of the UNT System Information Security Program shall review the Program for compliance with the DIR Security Controls Standards Catalog in accordance with 1 TAC §202.76(c).

Organization

Individuals fulfilling the following roles at or on behalf of the System Administration and each Institution shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1000, 1 TAC §§ 202.70 - 202.77, and Roles and RACI.

a. Executive Management

i. System or Institution Head or Designated Representative

The Chancellor of 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.

ii. Vice Chancellor and Chief Information Officer

The System Vice Chancellor and Chief Information Officer (VC/CIO) shall be responsible for approval, oversight, and coordination of the Information Security Program for the System Administration and Institutions.

iii. Associate Vice Chancellor and Chief Information Security Officer

The CISO is responsible for developing and administering the operation of the Information Security Program, providing leadership, strategic direction, and coordination for the UNT System Information Security Program, including issuing policies, standards, procedures, and guidelines.

iv. Information Security Officer

The Chancellor or VC/CIO shall appoint an Information Security Officer (ISO) for the System Administration. The President of each Institution or their 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 CISO for all security-related matters. The ISO shall evaluate security controls in terms of maturity and ensure readiness and effective control implementation.

v. Information Resources Manager

The individual who is designated by the agency to be responsible for overseeing information technology, information technology reporting, and technology compliance.

vi. Chief Technology Officer

The individual who is responsible for managing the physical and personnel technology infrastructure including technology deployment, network and system management, integration testing, and developing technical operations personnel.

b. Data/Information Management

i. Information Owner

The Information Owner is the person with operational authority for specific information and who is responsible for authorizing the controls for the 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.

ii. Information Steward

The delegate of the Information Owner responsible for granting and revoking access to institutional information and granting and revoking permission for the use of institutional information.

iii. Data Management Officer

The Data Management Officer is responsible for establishing an institutional data governance program, identifying the institution’s data assets, and establishing related processes and procedures to oversee the institution's data assets in accordance with state law.

c. 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 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 and any third party acting as an agent of, or otherwise on behalf of, the System Administration or an Institution. Custodians include but are not limited to:

i. Information Resource/Application Owners

Custodians who are responsible for the development, procurement, integration, modification, operation and maintenance, implementation of the Information Owner-defined controls, and/or final disposition of an information system.

ii. Network Administrators

Custodians responsible for managing networks within an organization and ensuring network security.

iii. System Administrators

Custodians responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established policy and procedures.

iv. Helpdesk Personnel

Custodians responsible for providing information and support for computing devices and their Users.

v. Third Parties

Individuals affiliated with one or more institutions of the UNT System in a contractual capacity with responsibilities for development, integration, modification, operation and maintenance, and implementation of Information Owner-defined controls.

d. 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. Users include but may not be limited to:

i. Faculty

Users classified as employees having academic rank in one or more Universities of the UNT System.

ii. Staff

Users employed part-time, full-time, or in a temporary capacity. Staff employees do not include faculty or employees under contract.

iii. Students

Users who are currently enrolled at one or more Universities of the UNT System.

iv. Alumni

Users who have earned a degree from one or more Universities of the UNT System.

v. Retiree

Users who left active employment with one or more institutions of the UNT System upon reaching TRS eligibility for retirement.

vi. Service Accounts

A digital identity used by a software application or service to interact with software applications or operating systems.

vii. Guests

Visitors to one or more institutions of the UNT System.

Privacy and Confidentiality

a. Requirements

UNT System 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, GLBA, and the Red Flags Rule

b. Responsibilities

i. Information Owners and Information Stewards must limit the collection, use, processing, and disclosure of Personal Identifying Information and Confidential Information to that which serves to meet its function and purpose.

ii. Custodians should restrict the use of Personal Identifying Information and Confidential Information to the purpose for which it was collected.

iii. Information Owners and Information Stewards should maintain accurate Personal Identifying Information and Confidential Information and exhibit a reasonable effort to keep the information up to date.

iv. Information System/Application Owners should keep Personal Identifying Information and Confidential Information no longer than necessary for processing as it was originally collected.

v. Information System/Application Owners should process and protect Personal Identifying Information and Confidential Information with security controls proportional to the information's confidentiality.

vi. The Information Owner or Information Steward must provide consent prior to the processing of special kinds of Personal Identifying Information and Confidential Information; including but not limited to genetic information, biometric information, and health information.

vii. Information System/Application Owners shall not process Personal Identifying Information and Confidential Information except under permissions granted by the Information Owner or Information Steward.

vii. Information Owners and Information Stewards must obtain an individual's written or electronic consent before acquiring, retaining, or disseminating information about an individual that identifies the individual or their location, including global position system technology, individual contact tracing, and biometric information except as required by law. The institution must maintain any records of consent agreements until the contract permitting the acquisition, retention, or dissemination of information expires.

c. Privacy and Institutional Websites

i. Custodians responsible for websites must post the following on websites that process Personal Identifying Information:

1. The types of data collected when visiting the website;

2. How collected information is used;

3. How collected information is protected, and

4. Whether collected information is shared.

ii. Custodians must conduct a transaction risk assessment prior to providing access to information or services on a website that requires Personal Identifying Information. Web Developers must implement privacy and security safeguards on websites that transmit, collect, or store Personal Identifying Information.

iii. Custodians must include links to the institution's Privacy policy on key website entry points.

iv. Custodians must include the following text on websites: "By using or accessing a university website you consent to allow 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."

v. The CISO and delegates must create a privacy notice that describes applicable provisions of the institutional privacy policy. The notice must meet the requirements of 1 TAC § 206.72.

vi. Custodians responsible for websites must publish the privacy notice on all key public entry points or site policy pages.

d. Website and Mobile Application Development

i. The developer of a UNT System web application, web form, or mobile application that processes Confidential Information must submit the information listed below to the CISO or their delegate for assessment:

1. A description of the web application, web form, or mobile application architecture,

2. The authentication mechanism for the web application, web form, or mobile application,

3. The administrator-level access to data included in the web application, web form, or mobile application, and

4. A security and privacy plan to establish planned beta testing of the web application, web form, or mobile application.

ii. The developer of a web application, web form, or mobile application that processes sensitive personal information, Personal Identifying Information or Confidential Information must subject the web application, web form, and mobile application to vulnerability and penetration testing and address any vulnerability identified before deployment.

Information Classification and Handling

a. Categories of Information

Information Owners and Information Stewards shall use the following information classification system to categorize information for risk assessments, make risk management decisions, establish controls, and protect information:

i. 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.

1. Information System/Application Owners and Custodians of information resources must label and protect Confidential Information.

2. Confidential Information must not be released or made available or accessible to unauthorized individuals.

3. Some Confidential Information including, but not limited to, Classified Information, Export Controlled Information, Controlled Unclassified Information, and Federal Tax Information are subject to elevated security requirements and all Users and Custodians must protect this information in accordance with those requirements.

ii. Proprietary Information not publicly available and proprietary to an institution that is controlled prior to release under the Texas Public Information Act with moderate requirements for confidentiality, integrity, or availability.

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

b. Information Safeguards

i. All members of the UNT System community must protect Institutional information in accordance with this Handbook and the UNT System Information Security Program.

ii. All members of the UNT System community must not collect, store, use, or process Personal Identifying Information or Confidential Information without justifiable business need and must ensure its protection in accordance with the Information Security Program.

iii. A department must consult with the CISO or their delegate to identify security requirements and develop risk mitigation plans for new information technology hardware, software, or systems development services that store or process Confidential Information, integrate with critical information resources, or present as a Moderate or High Impact Information Resource prior to purchase.

iv. UNT System Procurement is responsible for ensuring that obligations for adhering to information security requirements are included in contracts and other written agreements with third parties. Third parties are required to adhere to identified information security requirements.

v. Information Owners and Information System/Application Owners must establish and enforce the Principle of Least Privilege when developing standards, procedures, or assigning access permissions.

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

vii. Custodians and Project Leaders are responsible for ensuring that data are protected in accordance with data classification identified in this Handbook upon initiation of an information resource technology project.

viii. Custodians of information resources, including external parties providing outsourced information resource services, must implement physical, technical, and procedural safeguards for information resources that are commensurate to the criticality of the information system and classification of data used or processed in the information resource or services.

ix. Information Owners and System Application Owners must dispose of electronic records, devices, and media according to institutional policies and by employing sanitization methods with strength and integrity in proportion to the security classification and confidentiality of information.

x. Information systems accessible to the public must not store or process Confidential or Proprietary Information.

xi. Custodians that administer websites should review information posted to publicly accessible systems at least annually to ensure neither Confidential Information nor Proprietary Information is included.

xii. Custodians and Project Leaders must consult with the CISO or delegate during software engineering, development, and throughout the system lifecycle.

xiii. Upon the initiation of any information resource technology project or application development, the Information System/Application Owner and Project Leader must:

1. Classify any institutional data created or used in the project,

2. Determine and assign the appropriate security controls for the data, and

3. Determine the retention requirement for each classification.

xiv. Information System/Application Owners must protect Personal Identifying Information and Confidential Information and conduct a risk assessment prior to use to establish appropriate controls.

xv. Information System/Application Owners and Custodians must minimize use of Personal Identifying Information or Confidential Information during testing, training, and research purposes to only that which is needed to meet stated objectives. Information System/Application Owners and Custodians must also limit the quantity of Personal Identifying Information or Confidential Information collected, stored, or processed to samples that are needed to validate a stated purpose during testing, training, and when conducting research.

c. Asset Management

i. Information Owners and Information System/Application Owners must manage information and information resource assets in accordance with the requirements of this Handbook.

ii. Information and Information Resource Owners must identify and classify information and information resource assets and shall identify Owners, Custodians, and Users.

iii. Information System/Application Owners must assess information resource assets for risk and manage assets through the system development life cycle.

iv. Asset Inventories

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

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

3. Custodians must maintain a documented inventory of institutionally owned physical assets and software assets associated with information processing.

4. Custodians and Information Owners must conduct and maintain inventories of information resources that collect, use, maintain, and/or share Confidential Information or Personal Identifying Information and must document data flow mapping, how data are transmitted, storage locations of Confidential Information, and critical information system components.

5. The CISO or delegate is responsible for reviewing the institution's inventory of information systems and related ownership and security responsibilities.

Control Oversight and Safeguard Assurance

a. The CISO or their delegate shall evaluate security controls across the System Administration and Institutions in terms of maturity, scope and breadth of implementation, effectiveness, and associated deficiency to ensure readiness and effective control implementation.

b. The CISO or their delegate will work with Information System Administrators and System/Application Owners to develop Plans of Actions and Milestones for deficient controls found in information systems.

c. Information System/Application Owners of critical services and systems must develop and annually update a security and privacy plan for those services.

d. Operating System Control Oversight

    i. Information System/Application Owners must develop procedures that govern access to operating systems of institutionally owned computing devices and servers to ensure that no single person can access, modify, or use assets without authorization or detection.

    ii. Information System/Application Owners must control access to operating systems by a secure log on procedure.

    iii. Information System/Application Owners must ensure the use of logon banners that display to Users during the logon process specifying User rights and responsibilities regarding system usage.

    iv. Information System/Application Owners are responsible for adhering to the requirements of the Account Management section of this Handbook regarding

limiting the use of administrator and privileged access and must maintain documented access authorization with sufficient business need for such access.

v. Information System/Application Owners must review authorizations for privileged access rights at regular intervals and must document changes to privileged accounts.

vi. Users may not employ tools or utilities capable of overriding system controls without permission from Custodians.

vii. Administrator accounts or accounts with expanded privileges should only be used for the configuration of systems, execution of administrative tasks, and for the carrying out and correction of security actions.

viii. Information System/Application Owners must only grant shared administrator accounts or accounts with expanded privileges based on a justifiable need. Information System/Application Owners and System Administrators must implement controls to mitigate the risk arising from the use of shared administrator accounts or accounts with expanded privileges.

ix. Information System/Application Owners must verify the identity of a User prior to the activation of an administrator account or an account with expanded privileges.

x. End-Users are not authorized to hold privileged or administrative User roles within information systems.

xi. Individuals authorized to use 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.

xii. Custodians must change default vendor authentication information following installation of systems or software.

xiii. Individuals who hold administrator accounts or accounts with expanded privileges must adhere to the System Administrator Code of Ethics as referenced in Appendix A of this document.

xiv. Administrative or privileged account password composition and complexity must meet or exceed the security requirements established in the Identification and Authentication section of this Handbook.

xv. System Administrators should define and impose time parameters for session termination.

e. Application Control Oversight

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

ii. Information System/Application Owners must track licenses for applications that are limited by quantity to control unauthorized copying and distribution, as applicable.

iii. Information System/Application Owners must control and document the use of peer-to-peer file-sharing technology to prevent unauthorized distribution or reproduction of copyrighted work. Users may not employ tools or utilities capable of overriding application controls.

iv. Information System/Application Owners must log or document access to High Impact Information Resources.

v. Information System/Application Owners and System Administrators must only grant shared administrator accounts or accounts with expanded privileges based on a justifiable business need. System Administrators must implement controls to mitigate the risk arising from the use of shared administrator accounts or accounts with expanded privileges.

vi. Information System/Application Owners must verify the identity of a User prior to the activation of an administrator account or an account with expanded privileges.

vii. 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.

viii. Custodians must change default vendor authentication information following installation of systems or software.

ix. Administrative or privileged account password composition must meet or exceed the minimum requirements established in the Identification and Authentication section of this Handbook.

x. Information System/Application Owners must review authorizations for privileged access rights at regular intervals and must document changes to privileged accounts.

xi. Information System/Application Owners should define and impose time parameters for session termination.

xii. System Administrators should authorize access through internal connections by resource type, and documented according to the interface characteristics, security requirements, and information classification.

xiii. Custodians must comply with the requirements of the Information Security Program when testing data or managing test, development, and quality assurance environments.

f. Information Control Oversight

i. Information Owners and Information System/Application Owners must restrict access to data according to the Principle of Least Privilege.

ii. Information Owners and Information System/Application Owners must log or document access to Confidential Information.

iii. Office areas and computer screens should remain clear of Confidential Information when a device or office is unattended.

iv. Confidential Information should never be left unattended on media such as printers, fax machines, and other devices.

v. All members of the UNT System community should lock away Confidential Information that is in print format or stored on portable media when not in use or when an office is vacant. Physical media includes, but is not limited to tablets, phones, computers, removable storage devices, and printed information.

vi. Members of the UNT System community may not use photocopiers, scanners, digital cameras, or other reproduction technology for unauthorized duplication of Confidential Information.

vii. Users must not access, process, or store institutional information using unauthorized software or services.

g. Computing Device Control Oversight

i. System Administrators are responsible for providing the following support to computing devices:

1. Installing current versions of endpoint protection and encryption software on all newly acquired laptops prior to deployment;

2. Ensuring desktop and laptop computers receive updates and patches;

3. Investigating laptop computers that appear to have improperly functioning endpoint protection and documenting any variances from compliance; and

4. Resolving variances from compliance that fall within their support responsibilities.

ii. Custodians must install centrally administered vulnerability management tools as new information resources are deployed.

iii. System Administrators must seek a security exception for any variance to compliance with these requirements.

Information Security Risk Management

a. The CISO or their delegate is responsible for the assessment and evaluation of risk within the information resources and technology to ensure that business operations are capable of delivering programs and services efficiently and effectively within acceptable tolerances for potential negative outcomes.

b. The expense of security safeguards shall be in proportion to the value of the assets, the criticality of the data, and the inherent liability in failure to meet regulations, laws, contractual obligations, or other agreements to reduce or mitigate risk to those assets.

c. The VC/CIO will commission a system-wide security risk assessment of information resources consistent with UNT System enterprise and information technology risk frameworks.

d. The CISO or their delegate shall conduct risk assessments of High Impact information resources annually.

e. The risk assessment process must evaluate inherent risks of deficiencies in controls and continuously apply mitigating or compensating controls to reduce the residual risk to an acceptable level for the institution.

f. Risk assessments must use a standard methodology compatible with 1 TAC § 202.75. The CISO shall approve the treatment of low or moderate risks using a defined and documented plan. The Chancellor of the System Administration or the President of each Institution shall approve the treatment of high risks.

g. The Chancellor of the 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 accepting exposures or protecting the data according to its value and sensitivity.

h. Supply Chain Risk Management

The CISO or their delegate must develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems, system components, or system services.

i. Security Exceptions

i. The CISO or their delegate must implement procedures for granting and documenting security exceptions that incorporate the requirements of 1 TAC §§ 202.71, 202.72.

ii. The CISO or their delegate, with the approval of the institution of higher education head or their designated representative, may issue exceptions to information security requirements or controls.

iii. The custodial department must submit a request for a security exception if they cannot meet the requirements of this Handbook. Security exception requests must be submitted to the CISO or their delegate and include the following:

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

2. The service and asset tag numbers of the Information Resource.

3. Location of the Information Resource.

4. Current use of the Information Resource.

5. Reason why the variance cannot be resolved.

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

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

iv. The CISO or their delegate will coordinate exceptions and compensating controls with Information Owners and Information System/Application Owners.

v. The CISO or their delegate shall justify, document, and communicate any such exceptions as part of the risk assessment process and include risks on the risk register.

vi. The CISO or their delegate will approve or reject a request for a security exception and may revoke security exceptions at any time.

Security Compliance and Regulatory Requirements Management

a. All members of the UNT System community must comply with information protection laws and standards in regard to the use of 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 Administrative Code Title 1 Part 10 Chapter 202 for higher education institutions, 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.

b. Information Owners and their designees 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.

c. Custodians are responsible for implementing information security controls based on information protection laws and standards identified by Information Owners.

Cloud Usage and Security

a. Third parties entering into a written agreement with the System Administration or an Institution that provisions access to information technology agree to maintain the confidentiality, integrity, and availability of information owned by the System Administration or Institution

b. Third parties providing a Cloud Computing Service to the System Administration or an Institution must participate in and maintain compliance with the requirements of the State of Texas Risk and Authorization Management Program (TX-RAMP). The System Administration and Institutions may not enter into a new contract or renew an existing contract with a cloud computing provider with a third party that is not in compliance with TX-RAMP requirements.

c. The System Administration and Institutions at reasonable times throughout the terms of a contract may request supporting documents for the purpose of assessing and identifying risks posed by the relationship with a third party providing cloud computing services.

Security Assessment and Authorization

a. Information System/Application Owners and Project Leaders must ensure the performance of risk, security, and architectural assessments prior to the implementation, deployment, and acquisition of information resources.

b. Information System/Application Owners must ensure that security reviews are conducted to ensure the environment meets security requirements established by the UNT System Information Security Program.

c. The VC/CIO and their delegates are authorizing officials for information systems utilizing common controls for inheritance.

d. Information System/Application Owners must periodically review security and continuity documentation to ensure resiliency of services throughout the information resource life cycle.

e. Information System/Application Owners must submit information resources for risk, security, and architectural review at least every three years, or when significant changes occur.

Third Party Providers

a. UNT System Procurement is responsible for ensuring that obligations for adhering to information security requirements are included in contracts and other written agreements with third party service providers. Third parties are required to adhere to identified information security requirements.

b. Prior to entering a contract, third parties must submit:

    i. Evidence of compliance with applicable federal and state data protection and privacy laws including, but not limited to, the following: Family Educational Rights and Privacy Act, Health Information Portability and Accountability Act, Gramm-Leach-Bliley Act, and Export Control laws, and provide evidence of compliance with payment card industry data security standards if processing payments, as applicable.

    ii. Evidence that information systems provisioned for use by members of the UNT System community are designed and configured to adhere to State of Texas requirements for secure architectural design.

    iii. Architectural designs of applications, information systems, and websites

    iv. System diagrams of information systems in the context of the service that is being provided to the System Administration and Institutions.

    v. Evidence that information stored in third-party systems is recoverable and contingency plans are in place.

vi. A security assessment of the information resources and services provided to the System Administration or Institution.

c. UNTS responsibilities for third party lifecycle management

i. Authorizing Officials must monitor and maintain the lifecycle of all third parties with access to information and information resources, including but not limited to:

1. Access control;

2. Account management;

3. Reviewing access, permissions, and privileges assigned to third parties;

4. Ensuring the return of all confidential and proprietary information and information resource assets, and

5. Ensuring the removal of computer access when obligations or responsibilities of a third-party change.

ii. As part of the annual risk assessment process, Custodians shall require reviews of contracted third-party services to ensure continued compliance with agreed-upon security and compliance standards.

d. Third party service provider security and compliance requirements

i. Third parties acting as administrators, providers, or Custodians of Information Resources that are owned by the System Administration or Component Institutions must adhere to the requirements established in this Handbook and the UNT System Information Security Program, including requirements of the Texas Cybersecurity Framework and DIR Catalog.

ii. Adhere to service level agreements identified in contractual and written agreements with the System Administration or Institution for which the third party is providing a service or support.

iii. Implement remedial information security actions to adequately address non-compliance issues or risks identified during risk assessment processes, as a requirement of TX-RAMP, and throughout the system development lifecycle.

iv. Provide administrator access levels to data that will be processed within information systems.

v. Provide reports on security performance within the context of the contracted services.

vi. Report data breaches to the CISO within 48 hours of discovery and provide evidence of remediation.

vii. Provide authentication mechanisms for information systems and applications that comply with the requirements of the UNT System Information Security program

Enterprise Architecture, Roadmap, and Emerging Technology

a. The CTO shall develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

b. The CISO and delegates shall establish standards for the secure development of software, systems, and architecture that include the following:

i. Security of the development environment;

ii. Security in the software development methodology;

iii. Secure coding guidelines for each programming language used;

iv. Security requirements in the design phase;

v. Security checkpoints within the project milestones;

vi. Secure repositories;

vii. Security in version control;

viii. Required application security knowledge;

ix. Developers' capability of avoiding, finding, and remediating vulnerabilities; and

x. Planning for addressing end of support by the vendor.

Secure System Services, Acquisition, and Development

a. Information System/Application Owners and System Administrators are responsible for maintaining the security of systems and keeping software up to date.

b. Information Resource/Application Owners are responsible for developing security and privacy plans for information resources under their ownership prior to deployment. Security and privacy plans should include consideration of networks, facilities, systems, information, and other information resources.

c. Information System/Application Owners must design applications and information systems to align with the enterprise framework and must include security requirements in base architecture during information technology development, acquisition, and deployment.

d. 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 CISO or their delegate.

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

f. Employees of the System Administration and Institutions are prohibited from procuring Prohibited Technologies and must not install Prohibited Technologies on any institutionally issued device including, but not limited to: Desktops, laptops, cellphones, or any other computing or mobile device, in accordance with UNT System Regulation 06.1000 Information Security.

g. Only the System or Institution Head may issue exceptions to these requirements for legitimate business purposes and to accommodate student use of a System-issued email address. See UNT System Regulation 06.1000 Information Security for additional requirements concerning exceptions to these requirements.

Security and Privacy Awareness Training

a. Prior to Employment and Delivery of Services

   Supervisors and Department Heads must ensure that employees and third parties receive security and privacy awareness training and must inform employees and third parties about security policies and procedures during the onboarding process and prior to granting access to information resources.

b. During Employment and Delivery of Services

   i. Employees and third parties must complete:

1. Annual certified security and privacy awareness training designated by the CISO.

2. Role-based training as appropriate for role and responsibilities.

ii. Supervisors shall ensure that employees complete training for the handling of sensitive and Confidential Information as appropriate for their role.

iii. Employees must complete training supporting their information technology responsibilities and job duties in accordance with State of Texas requirements, including but not limited to continuing education.

iv. Employees must retain training records as required by retention schedules.

v. Individuals designated by the Texas Department of Information Resources as Information Resource Employees must complete the number of Continuing Education credits required for their IRE level designation. IREs should retain proof of participation for each educational activity.

Cryptography

a. Information Owners, Information System/Application Owners, and System Administrators must implement encryption requirements for authentication, information storage devices, data transmission, portable devices, removable media, and encryption key standards based upon documented risk management decisions or as required by external security requirements.

b. All members of the UNT System Community must encrypt Confidential Information transmitted over a public network in accordance with established standards.

c. Custodians should assess the risk of Confidential Information at rest and apply cryptographic controls as applicable or to meet external security requirements.

d. System Administrators must encrypt institutionally owned mobile devices. If a device is not capable of encryption, no Confidential Information may be stored on the device.

e. Custodians must encrypt Confidential Information that is stored in a public location directly accessible without compensating controls.

f. All members of the UNT System community must encrypt Confidential Information if copied to or stored on a portable computing device, removable media, or non-agency owned computing device.

g. Custodians must implement compensating electronic controls to secure a device that cannot be encrypted. The CISO must approve the compensating controls.

h. System Administrators must be able to document and verify the encryption of a device.

i. Administrators of key management systems are responsible for ensuring that encryption keys are securely managed.

Secure Configuration Management

a. Information Resource/Application Owners and System Administrators must implement configuration management processes for controlling modifications to hardware, software, firmware, and documentation.

b. System Administrators must document and implement baseline configurations for all network devices and information systems.

c. System Administrators must use the established change control and configuration management procedures for the review and approval of changes to baseline configurations to ensure compliance.

d. System Administrators must configure the system to provide only essential capabilities and only allow the ports, protocols, and applications necessary to support the business function of the information system.

e. System Administrators and Information System/Application Owners may only install authorized software on institutionally owned computing devices and servers.

f. Users are prohibited from installing unauthorized software on their institutionally owned computing device or integrating unauthorized software with UNT System Information Resources.

g. System Administrators must prohibit or restrict the use of Prohibited Technologies in standard configurations.

h. Equipment Maintenance

    i. Custodians must maintain equipment in accordance with the vendor's recommended service intervals and specifications.

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

    iii. Custodians should keep records of all preventative and corrective equipment maintenance and of all suspected or actual equipment errors.

iv. Custodians should implement controls when equipment is scheduled for maintenance, considering whether this maintenance is performed by personnel onsite or external to the organization. Where necessary, Custodians should clear Confidential Information from the equipment, or ensure the maintenance personnel have appropriate authorization.

v. Custodians should assess the risk prior to the implementation of vendor or service provider maintenance recommendations. Custodians must implement compensating controls or security exceptions if it is not possible to follow vendor or service provider maintenance recommendations.

vi. Custodians must inspect and test equipment prior to placing in operation to ensure integrity and proper function, and to verify that all potentially impacted security controls are intact.

vii. Custodians must monitor and approve maintenance activities and ensure that explicit approval is obtained prior to removing equipment.

Change Management

a. Custodians must implement change management procedures for Moderate and High Impact Information Resources that include security impact analysis, risk assessment with likelihood of success, significance to business resources required, business justification, testing changes prior to deployment, change deployment plan, guidance for change prioritization, and communication to affected Users, prior to deployment of changes.

b. Custodians must enforce physical and logical system access restrictions to permit only qualified and authorized individuals to initiate changes.

c. For each change, Custodians must perform and retain evidence of pre-deployment and post-deployment testing to ensure performance of the appropriate level of testing and business and/or IT stakeholders provide signoffs.

d. Change managers must monitor the implementation of a change to ensure security requirements are met throughout the lifecycle of the change.

Contingency Planning

a. Information System/Application Owners shall develop and maintain business continuity and disaster recovery plans for Moderate and High Impact 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.

b. Business continuity and disaster recovery plans must include:

    i. Information security protocols to ensure resiliency and system availability.

    ii. Alternate communication protocols in support of maintaining continuity of operations.

    iii. a business impact analysis to evaluate the impact of interruption to business operations,

    iv. a risk assessment to evaluate potential weaknesses, and

    v. documented system dependencies for developing the order of recovery, and recovery time objectives and recovery point objectives.

c. The VC/CIO must review and approve the business continuity and disaster recovery plan for High Impact enterprise information resources.

d. The CISO or their delegate shall coordinate with Information System/Application Owners to ensure sufficient planning, testing, reporting, and storage of business continuity and disaster recovery plans of High Impact Resources.

e. The CISO or their delegate shall distribute business continuity and disaster recovery plans for information resources to key personnel and store copies offsite.

f. The CISO or their delegate shall ensure business continuity and disaster recovery plans for High Impact Resources are tested at least annually.

g. Information System/Application Owners of High Impact Resources must update business continuity and disaster recovery plans after annual testing and as frequently as needed to reflect changes in the system or process.

h. Employees must receive training in their contingency roles and responsibilities with respect to the information system and complete periodic refresher training as necessary.

i. Information System/Application Owners are required to perform annual testing of redundant and high-availability information resources to ensure failover configurations work as intended.

j. The CTO or their delegate must define back up processes to protect the confidentiality, integrity, and availability of information stored in High Impact information resources.

k. Information System/Application Owners must regularly back up and test information contained in High Impact information resources.

l. Custodians must back up information from critical systems on a regularly scheduled basis consistent with agency recovery point objectives and store it logically and physically separated from the production environment.

m. The CTO or their delegate must establish alternate telecommunications services to permit the resumption of operations for essential functions when the primary telecommunications capabilities are unavailable.

Media

a. All members of the UNT System community must protect physical media containing information in accordance with the requirements established herein and as required in applicable laws, regulations, or standards.

b. Custodians must securely manage removable media and are responsible for ensuring appropriate encryption, storage, transport, and destruction commensurate with the value and sensitivity of the information stored.

c. Users must obtain access rights and authorizations from the Information owner prior to copying Confidential or Proprietary information to physical media.

d. Custodians must maintain strict protection controls over media containing Confidential or Proprietary Information and must protect the information and any devices or media against unauthorized access, misuse, and corruption during transport.

e. Custodians and Users must employ security controls to ensure the confidentiality, integrity, and availability prior to storing data on removeable media.

f. System Administrators must prohibit the use of portable media in information systems when the media has no identifiable owner.

Physical and Environmental Protection

a. Secure Areas

    i. Administrators of Secure Areas must document and manage physical access to ensure confidentiality, integrity, and availability of information resources, including verifying and monitoring access authorizations.

ii. Administrators of secure areas must collect and maintain records concerning the entrance and exit times of all individuals, including visitors.

iii. Administrators of secure areas must maintain access records in accordance with institutional retention policies.

iv. The administrator of a Secure Area must ensure that the facility is protected with emergency, environmental, and physical controls 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.

v. The administrator of a Secure Area must monitor and document delivery and removal of system components entering and exiting the Secure Area.

vi. Employees must protect work areas in accordance with physical controls and security requirements appropriate for the type of operational functions performed in the area.

vii. The administrator of a Secure Area must monitor physical access and coordinate results of reviews and irregularities with the CISO or their delegate.

viii. The administrator of Secure Area must document, test, and review physical security and emergency procedures for information resources as part of the risk assessment process.

ix. The Information Security Officer and administrator of a Secure Area shall only grant access to on-site personnel in accordance with job responsibilities.

x. Supervisors must monitor personnel working in Secure Areas. 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 mitigate identified applicable risks.

xi. The administrator of a Secure Area is responsible for ensuring that the area is locked, secured, and periodically inspected.

xii. 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.

b. Equipment Security

    i. Custodians must document, update, and test at least annually, procedures protecting High Impact information resources from environmental hazards, power failures, and other disruptions.

    ii. Administrators of secure areas shall ensure that employees who work in the area or provide support within the area are trained to monitor environmental controls, have knowledge of environmental control procedures and equipment, and are aware of response protocols for emergencies or equipment problems.

    iii. Users should log off or protect unattended computers with a screen and keyboard locking mechanism controlled by a password, token, or similar authentication mechanism.

Personnel Security

a. Authorizing Officials must ensure that individuals responsible for agency information are identified and their responsibilities clearly defined.

b. Authorizing Officials must assign risk designations and require background screenings as appropriate for an individual's roles and responsibilities, prior to granting access to UNT System information and information resources.

c. All employees and third parties must understand their roles and responsibilities pertaining to information security and comply with the Information Security Program.

d. Users of UNT System information and information resources must acknowledge rules of behavior, including but not limited to:

    i. Complying with the Information Security Program.

    ii. Information usage restrictions for social media, social networking, and external site/application when using such sites for official duties or in the conduct of official business.

    iii. Posting UNT System information on public websites.

e. Supervisors, Information Owners, and Information Stewards are responsible for reviewing and modifying employee access to information and information resources when changes occur in employment status.

f. Information Owners, Information Stewards, and university officials responsible for hosting third parties are also responsible for reviewing and modifying access to information and information resources when changes occur to written agreements.

g. Termination, Changes of Employment, and Cessation of Services

    i. Departments must have exit procedures in place that ensure the following:

        1. The return of all Confidential and Proprietary information and information resource assets upon termination of employment, cessation of services, or cessation of written agreements.

        2. The timely removal of computer access when the employment status, contractual obligation, or responsibilities of an individual changes.

        3. 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.

    ii. The terminating employee's immediate supervisor and a third party's hosting department are 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.

    iii. An employee's former and new supervisors should manage changes in responsibilities of employment 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 the Principle of Least Privilege and as appropriate for the sensitivity of the position.

    iv. The immediate supervisor of an employee, whose employment status changes, shall notify the Information Owners and Custodians of information resources about the change as soon as possible.

Third Party Personnel Security

a. The Information System/Application Owners 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:

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

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

b. 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.

c. Custodians must document and approve remote maintenance and diagnostic connections in advance.

d. Custodians must use strong authentication to establish remote maintenance and diagnostic connections.

e. Custodians shall terminate remote access and diagnostic connection upon completion of remote system maintenance.

f. Remote maintenance and diagnostic activities must be consistent with the other security policies in this Handbook.

System Configuration Hardening and Patch Management

a. Information System Owners shall ensure that systems are configured in a manner that prevents unauthorized access, unauthorized use, and service disruptions.

b. Information System Owners shall establish configuration change control practices that include documenting the type of changes, reviewing proposed configuration changes, documenting configuration change decisions, and implementing approved configuration control changes through established change management standards.

    i. Custodians must ensure that multi-user information systems are assessed by the Information Security Officer to ensure compliance with security policies and to ensure that appropriate controls are in place prior to placing the information system into production and before configuration or other changes occur.

ii. Custodians must protect documents, procedures, and guidelines associated with administration or implementation of information systems from unauthorized disclosure. Such information includes:

1. Secure configuration, installation, and standard operating procedures,

2. Effective use and maintenance of security functions, and

3. Known vulnerabilities regarding configuration and use of administrative functions.

c. Custodians of information resources must manage information resources in a manner that ensures that updates and patch management practices ensure compliance with vendor 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:

i. Prioritization of patches and system updates;

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

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

iv. Patch monitoring for correct installation;

v. Problems shall be addressed as they occur;

vi. Contingency plans for handling emergency or critical updates; and

vii. End-of-life procedures to address older systems using one or more of the following approaches:

1. Decommission system

2. Upgrade to latest platform

3. Migrate to another platform

4. Manage risk through use of compensating controls

Access Control

a. Information System/Application Owners and System Administrators must establish and enforce the Principle of Least Privilege when developing standards, procedures, or assigning access permissions.

b. Information System/Application Owners should only authorize the connection of mobile devices through secure configuration requirements and connection requirements.

c. Access Authorizations

    i. Access authorizations must be established prior to granting employees and third parties access to institutional information and information resources.

    ii. Access authorizations shall include a signed acknowledgment that the User understands responsibilities and expected behaviors of accessing institutional information resources.

    iii. Information System/Application Owners and Information Owners are responsible for verifying third party access authorizations prior to granting access to UNT System information and information resources.

    iv. Access authorizations must be reviewed, modified, and acknowledged as changes are made to User responsibilities and expected behaviors.

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

d. Logon Banner

    As required by 1 TAC §202.72(b), all System Administration and Institution Information Resources must require the acceptance of a logon banner prior to use. The identification/logon banner shall include the following topics at minimum:

    i. Unauthorized use is prohibited;

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

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

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

v. 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.

e. Separation of Duties

i. Information System/Application Owners and Information Owners of Moderate and High Impact Information Resources must identify and document responsibilities of individuals requiring separation of duties for tasks susceptible to erroneous and inappropriate actions.

ii. System Administrators must define system access authorizations to support separation of duties.

iii. Information System/Application Owners must implement separation of duties for transactional High Impact Information Resources to prevent misuse, fraud, or other unauthorized activity.

f. User Responsibilities

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

ii. Users must keep their accounts, passwords, and authentication factors secure.

iii. Passwords must not be shared with anyone and are Confidential Information.

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

v. Users must adhere to all requirements of the Identification and Authentication section of this handbook.

vi. Users should only access information and use information resources required to perform job duties.

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

Account Management

a. Information System/Application Owners, System Administrators, Information Owners, and Information Stewards must 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, acknowledgment of User responsibilities, managing passwords, periodic access reviews, and prompt removal of access during role change or termination.

b. Information System/Application Owners, Information Owners, and Information Stewards must perform, at a minimum, quarterly access reviews of Users with access to Confidential Information and information resources that present as a high or moderate impact to the System Administration and Institutions.

c. Information System/Application Owners, Information Owners, and Information Stewards must perform annual access reviews for all information resources.

d. Information System/Application Owners and Information Owners shall restrict User access, including privileged access, to information and information resources according to the Principle of Least Privilege.

e. Information System/Application Owners must implement multifactor authentication for accounts with privileged access.

f. Information System/Application Owners must implement multifactor authentication for accounts with access to critical information resources or as required by law.

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

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

i. Information System/Application Owners must only grant privileged access to information resources to System Administrators of and not to end-users.

j. Information System/Application Owners, Information Owners, and Information Stewards shall grant, monitor, and review privileged access in accordance with the UNT System Information Ownership Guide and published access control standards.

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

l. Custodians will assign privileged access rights to a different User ID than those used for regular day-to-day activities.

m. Individuals with privileged access rights must have the appropriate skills and knowledge to securely administer technology and maintain the confidentiality, integrity, and availability of the information resources for which they are granted access. Individuals with privileged access rights must keep their skills and knowledge current to maintain privileged access.

n. Information System/Application Owners, Information Owners, and Information Stewards must revoke privileged access in the event of a violation of policy, procedure, or mandate.

o. Information System/Application Owners should avoid the use of default privileged accounts. If using default privileged accounts cannot be avoided, Information System/Application Owners must employ compensating controls to ensure the security of the information resource.

Network Access and Perimeter Controls

a. The CTO or their delegate must develop procedures for the secure management, access, monitoring, and control of institutionally owned and managed communications networks.

b. Information System/Application Owners must follow established standards and procedures that govern access, management, and monitoring of communication networks and devices.

c. Network Administrators must configure firewalls to block access of Prohibited Technologies to all UNT System technology infrastructures, including local networks, WAN, and VPN connections. Firewalls must also block personal devices with Prohibited Technologies from accessing UNT System and State of Texas technology infrastructures and data.

d. Network Administrators must implement the following requirements to ensure the secure management, access, monitoring, and control of institutionally owned and institutionally managed communications and networks.

    i. Network Administrators must restrict access to the network to authorized devices and Users.

    ii. Network Administrators must log or otherwise document network access;

    iii. Network access must adhere to the Principle of Least Privilege;

    iv. Networks must be segmented by function;

v. Network Administrators must implement appropriate security controls based on the criticality and value of the resources on the network;

vi. Networks must be monitored; and

vii. 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.

e. Network Connections

i. Only authorized users may connect to institutional networks.

ii. The introduction of network devices or information resources that negatively affect the behavior or security of the network or violate university policies, are prohibited.

iii. The CTO or their delegate must approve 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 prior to their introduction.

The following examples of types of devices require approval:

1. Multicasting

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

3. Devices that answer ARP requests as servers;

4. Network Security Appliances;

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

6. Routers;

7. Bridges;

8. Switches;

9. Proxy servers;

10. Wireless access points;

11. High bandwidth devices; and

12. Other similar devices.

iv. If a device on the network is found to compromise any aspect of the network's operation, System Information Technology, in coordination with the local IT support, may remove the device from the network.

Internet Content Filtering

The CISO or their delegate may establish controls to:

a. Block access to Internet websites based upon categories of content, application types and granular application functions, time of day or amount of utilization, or the dynamically updated reputation of the destination.

b. Preserve bandwidth by removing unnecessary bandwidth usage from the network by blocking access to sites that are not business related and consume excessive bandwidth.

c. Filter content to prevent the infection and spread of malware through Internet content.

Data Loss Prevention

a. Information Owners must implement data loss prevention practices to detect and prevent potential data breach incidents where sensitive may be disclosed to unauthorized personnel by malicious intent or inadvertent mistake, including detection of data at risk while in use at the endpoint, while in motion during transmission, and while at rest on data storage devices.

b. The CISO may employ data loss prevention tools for protecting institutional data in motion and data at rest.

Identification and Authentication

a. Information System/Application Owners must establish identification and authentication procedures for information resources that comply with the requirements of the UNT System Information Security program.

b. Information System/Application Owners and System Administrators must establish accounts that uniquely identify and authenticate Users to ensure all actions established by the User account are traceable and attributed to the User.

c. Information System/Application Owners of critical systems must document and provide supporting rationale in security plans for User actions that are permitted without

identification and authentication.

d. High Impact information resources, information resources that integrate with critical applications, and information resources that store Confidential Information must utilize enterprise identification and authorization mechanisms.

e. Information Resource/Application Owners may utilize enterprise identification and authentication mechanisms for information resources which present a low impact to the System Administration and Institutions.

f. Password Standards

   Passwords should meet or exceed the following standards for all systems owned or managed by the UNT System:

   i. Passwords must have a minimum length of 12 characters;

   ii. Passwords have a maximum length of 64 characters; and

   iii. Password complexity may include a combination of uppercase letters, lowercase letters, digits, and special characters.

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

h. Password expiration may be implemented based on business need, compliance requirement, elevated external security requirement, or in the event of compromise.

i. System Administrators must set password requirements to lock User accounts for a minimum of 15 minutes or more after 10 unsuccessful logon attempts for low or moderate impact systems and 5 attempts for high impact systems.

j. System Administrators must ensure password verification includes comparison against common dictionary words, passwords obtained from previous breach corpuses, repetitive or sequential characters (e.g., ‘aaaaa’, ‘1234abcd’), and context specific words, such as the name of the service, the username, and derivatives thereof.

k. System Administrators must set password requirements to limit the reuse of passwords up to 5 previously used passwords and must ensure passwords are compared against values known to be commonly used, expected, or compromised.

l. System Administrators must ensure authentication feedback is obscured during user authentication.

m. 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.

i. Custodians should change the credentials for any system or generic account from the default value supplied by the vendor before the system is placed in a production capacity or is put on a public network.

ii. Custodians must escrow credentials with their supervisors and backup personnel for generic privileged accounts for systems critical to business operations.

iii. Custodians must change passwords for shared or generic privileged accounts when an 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.

n. Administrative, privileged, and service account password composition that does not meet these requirements must have mitigating controls approved by the CISO or their delegate.

o. The CISO or their delegate may grant an exception if a system is unable to accommodate these requirements.

Portable and Remote Computing

a. The CTO or their delegate must develop and communicate secure remote access procedures to ensure the confidentiality, integrity, and availability of UNT System information and information resources.

b. Information System/Application Owners must provide secure remote access information resources that protect communications and UNT System data from unauthorized access and that detect changes to remote access communications occurring in transit.

c. Custodians and Users must utilize centrally administered remote access solutions when accessing Confidential or Proprietary Information from alternative work sites.

d. Users must adhere to security requirements of the Information Security Program, including this Handbook and associated procedures when using or accessing institutional information and information resources remotely.

e. Alternate work sites

i. Users should utilize institutionally issued computing equipment when working at an alternative work site.

ii. Users must use centrally administered remote communications resources.

iii. Users must ensure Confidential Information is encrypted when transmitted over public or untrusted networks.

iv. Users must encrypt all Confidential Information when transmitted through electronic mail.

v. Users working at alternative work sites must ensure physical and technical controls are in place prior to accessing information and information resources owned by the UNT System.

vi. Custodians and Users must utilize centrally administered remote access solutions when accessing Confidential Information or Proprietary Information from alternative work sites.

vii. Users must only save work-related files using UNT System approved and centrally administered storage services or methods.

viii. Users must ensure that computing devices meet institutional security standards for remote access, including but not limited to, maintaining current versions of endpoint protection or antivirus software.

ix. Users must ensure that all computing devices are patched regularly with respect to operating system and application updates.

f. Remote maintenance

i. System Administrators must document and approve remote maintenance and diagnostic connections in advance.

ii. System Administrators must use strong authentication to establish remote maintenance and diagnostic connections.

iii. System Administrators shall terminate remote access and diagnostic connection upon completion of remote system maintenance.

System Communications Protection

a. All members of the UNT System community must protect information exchanged with an external institution, agency, or organization 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.

b. Custodians must establish controls to ensure Confidential Information leaving UNT System is protected with encryption.

c. Information transfer agreements must govern the transfer of information to an external institution, agency, or organization to ensure the confidentiality and integrity of institutionally owned data. Information transfer agreements should include the following:

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

    ii. Procedures to ensure traceability and non-repudiation;

    iii. Minimum technical standards for packaging and transmission;

    iv. Escrow agreements;

    v. Courier identification standards;

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

    vii. 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;

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

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

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

    xi. Acceptable levels of access control.

d. System Administrators should authorize access to information through internal connections by resource type, and documented according to the interface characteristics, security requirements, and information classification.

Information Systems Currency

a. System Administrators must eliminate unsupported software and systems to ensure the delivery of reliable, low-risk, and cost-effective services.

b. System Administrators must monitor for end-of-life systems and applications to plan for mitigation and prevent future vulnerabilities.

c. System Administrators should include software replacement schedules in their technology planning before the software is no longer supported by the vendor or manufacturer.

d. The CISO and their delegates will conduct a high-level risk assessment of software currency and work with System Administrators to resolve unsupported software and systems.

e. Risk decisions must be documented and approved in accordance with this handbook.

f. Custodians must request a security exception from the Information Security Officer for systems that have reached end-of-life.

Vulnerability Assessment

a. System Administrators must follow vulnerability management standards which include acceptable time frames for addressing vulnerabilities and escalation procedures for handling unaddressed vulnerabilities.

b. The CISO or their delegate will use vulnerability scanning tools to perform scans of information technology systems to identify information security vulnerabilities.

c. System Administrators will identify vulnerabilities through active monitoring and review of third-party vulnerability sources for any old, new, or unique vulnerabilities that currently exist.

d. The Information Security Officer or delegate is the only official authorized to perform, approve, and initiate vulnerability assessments or penetration tests.

e. The Information Security Officer or validated third party will conduct penetration tests that identify vulnerabilities that threat actors might exploit.

f. The Information Security Officer will check each vulnerability alert and patch release against existing systems and services prior to taking any action to avoid unnecessary remediation.

g. The CISO 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 as described in the Vulnerability Management Standard.

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

i. The Information Security Officer will identify remediation options based on numerous risk factors including the availability of a patch and the risk accepted by utilizing a different method.

j. If remediation is not implemented Custodians will

    i. Implement compensating controls;

    ii. Follow the risk management process; or.

    iii. Pursue an exception.

k. Custodians must immediately update all configuration and inventory documentation to reflect applied remediation.

l. Custodians must not block authorized network scan source IP addresses on the devices they support.

Malware Protection

a. The CISO or their delegate shall establish procedures regarding malware, malicious, or unwanted programs which shall address malware on system, application, and network layers.

b. System Administrators must install centrally administered endpoint protection agents on all computing information resources managed by System Administration or Institutions.

c. System Administrators must keep endpoint protection in a current and supported state.

d. System Administrators must configure endpoint protection software so Users cannot disable or prevent the software from functioning properly.

e. The Information Security Officer shall ensure that automated tools are available to scan information resources for malware, malicious programs, or unwanted programs.

Security Monitoring and Event Analysis

a. The CISO or their delegate shall conduct analysis of security events and alerts as detected through the use of centrally administered vulnerability management and endpoint protection tools.

b. System Administrators must contact the CISO or their delegate to report activities that indicate a security incident has occurred.

c. Monitoring and logging functions must provide audit trails to ensure accountability for updates High Impact information, hardware, and software.

d. Custodians for enterprise systems should produce, maintain, and regularly review event logs that record User activities, exceptions, faults, and information security events.

Audit Logging and Accountability

a. Information System/Application Owners and System Administrators must follow established logging management standards to identify, respond, and prevent operational problems, security incidents, policy violations, and fraudulent activity.

b. Information System/Application Owners and System Administrators must establish controls to ensure the confidentiality and integrity of information in system logs, transaction histories, and other system audit information and must monitor and store this information in a location separate from the systems generating the information.

c. Information System/Application Owners and System Administrators must review logs and report findings of security incidents, policy violations, and fraudulent activity upon discovery to the CISO or their delegate.

d. 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.

e. System Administrators must alert System Information/Application Owners in the event of audit logging process failures and take action to resolve.

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

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

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

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

    iv. Information Owners, or their designees, and Custodians should allow read-only access for isolated copies of system files and should erase the files when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.

    v. Information Owners, or their designees, and Custodians should identify and agree upon requirements for special or additional processing.

vi. Information Owners, or their designees, and Custodians should run audit tests that could affect system availability outside business hours.

vii. Information Owners, or their designees, and Custodians should monitor and log all access, where appropriate, to produce a reference trail.

Cyber Security and Privacy Incident Response

a. All members of the UNT System community must comply with the Information Security Program to ensure the confidentiality, integrity, and availability of all UNT System information and information resources and must immediately report security incidents and suspected security incidents to the CISO or their delegate.

b. The CISO or their delegate must establish an incident response plan that complies with the requirements of 1 TAC 202 and the DIR Catalog and must annually test the effectiveness of the plan.

c. Management of Information Security and Privacy Incidents

i. The CISO or their delegate will assess the incident, oversee incident response, assemble incident response teams as necessary, and will coordinate incident handling, remediation, reporting, response, and the authorization of forensic analysis as necessary.

ii. Custodians, Information Owners, and Users must cooperate with incident investigations.

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

iv. The CISO or their delegate shall assist and advise information system Users in the handling and reporting of security incidents.

v. The CISO or their delegate shall employ automated mechanisms to increase the availability of incident response-related information and support.

vi. As required by 1 TAC § 202.73 the Information Security Officer must report information security incidents to the Texas Department of Information Resources. Incidents that propagate to other state systems, result in criminal violations, involve unauthorized disclosure or modification of Confidential Information, or result in the compromise, destruction or alteration of information resources must be reported within 48 hours. Summary reports of security incidents must be submitted monthly.

vii. All personnel involved in incident handling must maintain confidentiality of security and privacy incidents and associated activities during all phases of incident handling.

Acknowledgment of Security Responsibilities

All Users of information and information resources of the System Administration and Institutions, including faculty, staff, students, guests, contractors, consultants, and all third parties shall acknowledge and abide by the security controls governed by relevant legislative, statutory, regulatory, and contractual requirements.

Sanctions

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 the System Administration and Institutions.

Authority over the Information Security Program

The CISO has all authority to modify and enforce the UNT System Information Security Program, including but not limited to suspension of access, enforcement of security controls, and removal of resources from UNTS networks unilaterally or in consultation with UNTS officials.

The CISO has the sole discretion to make changes to the Information Security Program at any time and without advance notice.

Appendix A: Glossary

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

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

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

d. Business Continuity Planning. The process of identifying High Impact 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.

e. 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.

f. 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.

g. Cloud Computing Service. A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. Service models that represent cloud computing include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud computing services can be deployed in a private cloud, community cloud, public cloud, or hybrid cloud.

h. 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.

i. Custodian. A person responsible for implementing the Information owner-defined controls and access to information and information resources. Custodians are responsible for the operation of an information resource. Individuals who obtain,

access, or use information provided by Information Owners for 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.

j. 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.

k. Enterprise Information Resource. An information resource that is administered by UNT System Information Technology.

l. 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:

   i. 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;
   ii. Result in major damage to organizational assets;
   iii. Result in major financial loss; or
   iv. Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

m. Hosting Department. A department contracting with an external party that will require access to institutional information or information resources.

n. 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.

o. 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.

p. Information Resource/Application Owner. Custodians responsible for the development, procurement, integration, modification, operation and maintenance, implementation of the Information Owner-defined controls, and/or final disposition of an information system.

q. Information Security. The protection of information and information resources from threats 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.

r. Information Security Officer. The Information Security Officer is responsible for developing and administering the operation of an information security program. The VC/CIO, 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 VC/CIO for all security-related matters.

s. Information Security Program. The UNT System information security program includes the policies, Information Security Handbook, control catalog, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions. The information security program shall comply with applicable federal and state laws related to information resources and information security, including but not limited to 1 Texas Administrative Code §202, the Texas Cybersecurity Framework, and the State of Texas Department of Information Resources Security Controls Standards Catalog (DIR Catalog).

t. Information Steward. A delegate of the Information Owner responsible for granting and revoking access to institutional information and granting and revoking permission for the use of institutional information.

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

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

w. 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.

x. Low Impact Information Resource. Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

    i. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

ii. result in minor damage to organizational assets;
iii. result in minor financial loss; or
iv. result in minor harm to individuals.

y. Moderate Impact Information Resource. Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

i. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
ii. result in significant damage to organizational assets;
iii. result in significant financial loss; or
iv. result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

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

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

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

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

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

i. Name, social security number, date of birth, or government-issued identification number;
ii. Mother's maiden name;
iii. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
iv. Unique electronic identification number, address, or routing code; and
v. Telecommunication access device as defined by Section 32.51, Penal Code.

ee. Plans of Actions and Milestones. A corrective action plan roadmap to address system weaknesses and the resources required to fix them.

ff. Privileged Access. An escalated level of resource access that allows changes to information systems and can affect the confidentiality, integrity, or availability of information or information resources. Privileged access is granted to Users responsible for providing information resource administrative services such as system maintenance, data management, and User support.

gg. Prohibited Technologies. Any software or hardware products that are not permitted on System-Issued devices or networks, including but not limited to Alipay, ByteDance Ltd, CamScanner, Kaspersky, QQ Wallet, SHAREit, Tencent Holdings Ltd., TikTok, VMate, WeChat, WeChat Pay, WPS Office; Dahua Technology Co., Huawei Technologies, Co., Hangzhou Hikvision Digital Technology Company, Hytera Communications Corp., SZ DJI Technology Co., ZTE Corp; any subsidiary, affiliate or successor of these entities; and any software, hardware of entities identified and posted by the Texas Department of Information Resources at: Prohibited Technologies | Texas Department of Information Resources.

hh. Project Leader. The person responsible for the oversight of an information technology projects including an application development or any information resources project.

ii. Proprietary Information. Information that is proprietary to an Institution or has moderate requirements for confidentiality, integrity, or availability. Suggested definition – Information not publicly

jj. 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.

kk. Ransomware. Malicious code intended to lock and restrict access by an unauthorized person to a computer, computer system, or computer network or any data in a computer, computer system, or computer network when money, property, or a service is demanded to remediate the impact of the malicious code.

ll. 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).

mm. Recovery Time Objective (RTO). The duration of time and the 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.

nn. Remote Access. Access to an institutional information system by a User communicating through an external, non-organization-controlled network.

oo. 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.

pp. 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.

qq. 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.

rr. Secure Area. A physical location where critical, confidential, or sensitive technology assets or data are stored.

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

tt. Security 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 and include, but are not limited to, breaches, suspected breaches, and ransomware.

uu. Supply Chain Risk. The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.

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

ww. System Administrators. A Custodian responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established policy and procedures.

xx. 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.

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

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

aaa. 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.

Appendix B: System Administrator Code of Ethics

1. Introduction

    a. 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

    a. 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 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

    a. Users with elevated and broader-than- normal access to information resources agree:

    b. 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.

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

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

    e. Not to intentionally or recklessly damage or destroy any information or information resources.

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

g. 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.

h. 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.

i. 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.

j. 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.

k. 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.

l. Not to engage in any improper or deceptive financial practices.

m. Not to associate with malicious hackers, engage in or promote malicious activities that affect the confidentiality, integrity, or availability of information and information resources.

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

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

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

q. 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.

r. Conduct themselves in a manner that will foster security

awareness and understanding among Users.

s. Respect the rights of intellectual property ownership by adhering to copyright laws and institutional policy.
t. Follow the requirements and limitations of software licenses. Never use software that is obtained or retained either illegally or unethically.
u. Only perform authorized actions on information resources and adhere to the User access agreement.
v. Conduct their work using good project management, incorporating quality practices, and providing full disclosure of risk.
w. Conduct themselves ethically and professionally in the execution of their job duties.

Appendix C: Handbook References

1. State of Texas Laws, Regulations, and Requirements

    1.1. Texas Government Code Chapter 2054
    1.2. Texas Administrative Code, Title 1, Section 202
    1.3. Texas Cybersecurity Framework
    1.4. Department of Information Resources Security Controls Standards Catalog
    1.5. Texas Risk and Authorization Management Program Manual
    1.6. Model Security Plan for Prohibited Technologies

2. System Administration Policies, Regulations, and Publications

    2.1. UNT System Regulation 06.1000 Information Security
    2.2. UNT System Information Ownership Guide
    2.3. Access Control Standard
    2.4. Change Management Standard
    2.5. Vulnerability Management Standard
    2.6. Log Management Standard
    2.7. UNT System Information Security Mandate — Mobile Device Encryption
    2.8. Information Technology Mandate: SEC 1001 — Crowdstrike Endpoint Security Solution Compliance

3. Industry Standards and Guidelines

    3.1. NIST 800-63B
    3.2. NIST 800-46

4. Handbook Contributors

Name	Title	Institution
Juan Serrano	Vice Chancellor and Chief Information Officer	UNT System Administration University of North Texas University of North Texas at Dallas University of North Texas Health Science Center

Name	Title	Institution
Richard Anderson	Associate Vice Chancellor and Chief Information Security Officer	UNT System Administration University of North Texas University of North Texas at Dallas University of North Texas Health Science Center
Michael Hollis	Deputy Chief Information Security Officer and UNTHSC Information Security Officer	UNT System Administration University of North Texas University of North Texas at Dallas University of North Texas Health Science Center
Patrick McLeod	Business Information Security Officer	University of North Texas
Patrick Lampkin	Business Information Security Officer	University of North Texas System University of North Texas at Dallas
Paula Mears	Director of Security Operations	UNT System Administration University of North Texas University of North Texas at Dallas University of North Texas Health Science Center
Christine Sikes	Director of IT Governance, Risk, & Compliance	UNT System Administration University of North Texas University of North Texas University of North Texas at Dallas University of North Texas Health Science Center

Name	Title	Institution
Rachel Burlage	Information Security Analyst	UNT System Administration University of North Texas University of North Texas University of North Texas at Dallas University of North Texas Health Science Center

Appendix D: 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	06/03/2019	Information Security Handbook Working Group Final Review Changes
7	Charlotte Russell	08/31/2020	Information Security Handbook Working Group
8	Charlotte Russell	12/08/2021	Revisions to Section 15: Vendor Relationship; Information Security Handbook Working Group Final Review Changes
		01/19/2022	Chief Information Officer Revision
9	Richard Anderson	10/01/2022	Chief Information Officer Revision
10	Richard Anderson	12/04/2023	Align Information Security Handbook to Texas Cybersecurity Framework