UNT SYSTEM

Information Security Handbook

Adopted 6/4/14

1. Introduction

1.1. Executive Summary

The University of North Texas System Information Security Handbook establishes the information security program framework for the System Administration and Institutions. The UNT System is committed to establishing an information security program designed to protect the confidentiality, integrity, and availability of information and information resources. Implementation of an information security program supports business continuity, management of risk, enables compliance and maximizes the ability of the System Administration and Institutions to meet their goals and objectives.

1.2. Governance

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

1.3. Scope and Application

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

1.4. Biennial Review

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

2. Definitions

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

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

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

2.4. Business Continuity Planning. The process of identifying mission-critical information systems and business functions, analyzing the risks and probabilities of service disruptions and outages, and developing procedures to continue operations during outages and restore those systems and functions.

2.5. Category I Information. Information that requires protection from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, and judicial requirements), legal agreement, or information that requires a high degree of confidentiality, integrity, or availability. Category I information must be identified, documented, and protected.

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

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

2.8. Chief Information Officer. The senior information technology official for an Institution who is responsible for oversight of the information resources of that Institution. This position also acts as the State of Texas designated information resources manager.

2.9. Confidential Information. Information that must be protected from unauthorized disclosure or public release, based on state or federal law (e.g., the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

2.10. Custodian. A person responsible for implementing the information owner-defined controls and access to an information resource. Custodians are

responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by information owners for the purpose of performing tasks also act as custodians of the information and are responsible for maintaining the security of the information. Custodians may include employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the institution.

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

2.12. Enterprise Information Resource. An information resource that is administered by Information Technology Shared Services.

2.13. Incident. A security event that results in, or has the potential to result in a breach of the confidentiality, integrity, or availability of information or an information resource. Security incidents result from accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or modification of information resources or information.

2.14. Information Owner. A person with operational authority for specified information and who is responsible for authorizing the controls for generation, collection, processing, access, dissemination, and disposal of that information.

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

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

2.17. Information Security Officer. The Officer is responsible for developing and administering the operation of an information security program. The Associate Vice Chancellor for Information Technology or his or her designee shall appoint an Information Security Officer for the System Administration. The President of each institution or his or her designee shall appoint an Information Security Officer for the Institution. In addition to their administrative supervisors,

Information Security Officers will report to and comply with directives from the Associate Vice Chancellor for Information Technology for all security related matters.

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

2.19. Institution. A degree-granting component of the University of North Texas System.

2.20. Least Privilege. The security principle that requires application of the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

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

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

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

2.24. System Administration. The central administrative component of the University of North Texas System.

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

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

3. Structure of the Information Security Handbook

The structure of the information security handbook is consistent with the framework established in ISO 27001 and 27002. In addition, requirements of the handbook are consistent with the Information Security Standards established in 1 Texas Administration Code §§202 and 203, as amended.

3.1. Reference

3.1.1. University of North Texas System Information Security Regulation 6.1

4. Risk Management and Assessment

4.1. Purpose

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

4.2. Requirements

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

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

4.2.3. Risk assessments must use a standard methodology that is compatible with 1 TAC §202.72.

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

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

4.3. References

4.3.1. 1 Texas Administrative Code §202.72 Managing Security Risks
4.3.2. ISO 27002 Risk Assessment and Treatment

5. Information Security Policy

The System Administration and Institutions are required to adopt and implement information security programs, policies and processes that are consistent with the requirements set out in the Security Handbook and shall comply with the requirements of the Security Handbook. The Security Handbook will be reviewed and updated as needed. The System Information Security Officer will notify campus Information Security Officers if changes are made to the Security Handbook. A working group shall be assembled with representatives from the System Administration and each Institution to review and approve changes. The System Administration and Institutions should review security policies at regular intervals, make changes as needed and distribute to all appropriate parties.

6. Information Security Structure

6.1. Purpose

The responsibilities for managing information security are assigned to designated individuals within the organization and external to the organization. Officials of the System Administration and each Institution, as well as external entities, shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1, 1 TAC §202.70 and 1 TAC §202.71.

6.2. Internal Organization

The following officials at the System Administration and each Institution shall comply with their assigned responsibilities as specified in UNT System Security Regulation 6.1, 1 TAC §202.70 and 1 TAC §202.71.

6.2.1. System or Institution Head or Designated Representative

The Chancellor for the System Administration and the President of each Institution or their designee is responsible for overseeing the protection of information resources and for reviewing and approving the designation of

information owners and their associated responsibilities.

6.2.2. Associate Vice Chancellor for Information Technology

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

6.2.3. Information Security Officer

The Associate Vice Chancellor for Information Technology or his or her designee shall appoint an Information Security Officer for the System Administration. The President of each institution or his or her designee shall appoint an Information Security Officer for the Institution. The Information Security Officer is responsible for developing and administering the operation of an information security program. In addition to their administrative supervisors, Information Security Officers will report to and comply with directives from the Associate Vice Chancellor for Information Technology for all security related matters.

6.2.4. Information Owner

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

6.2.5. Custodian

The Custodian is the person responsible for implementing the information owner-defined controls and access to an information resource. Custodians are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by information owners for the purpose of performing tasks also act as custodians of the information and are responsible for maintaining the security of the information. Custodians may include employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the System Administration or an Institution.

6.2.6. User

A User is an individual or automated application authorized to access an information resource in accordance with the information owner-defined controls

and access rules.

6.3. External Organization

6.3.1. Access, permissions, and privileges assigned to vendors, consultants, and other persons of interest must be managed and reviewed to ensure the return of all confidential and proprietary information, information resource assets, and ensure the removal of computer access when the obligations or responsibilities of the external party change.

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

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

6.4. References

6.4.1. 1 Texas Administrative Code § 202.71, Management and Staff Responsibilities
6.4.2. ISO 27002 Organization of Information Security

7. Asset Management

7.1. Purpose

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

7.2. Responsibility for Information Assets

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

7.3. Information Classification and Handling

7.3.1. Categories of Information

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

7.3.1.1. Category I includes confidential information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, and judicial requirements), legal agreements, or information that requires a high degree of confidentiality, integrity, or availability. Category I information must be identified, documented, and protected.

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

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

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

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

7.3.4. The System Administration and Institutions must comply with 1 TAC §202.75(4)(A-D).

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

7.4. Information Safeguards

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

7.4.2. The System Administration and Institutions must dispose of electronic records and devices according to 1 TAC 202.78.

7.5. References

7.5.1. 1 Texas Administrative Code § 202.71(b) Management and Staff Responsibilities
7.5.2. 1 Texas Administrative Code § 202.78 Removal of Data from Data Processing Equipment
7.5.3. ISO 27002 Asset Management

8. Human Resources Security

8.1. Purpose

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

8.2. Prior to Employment

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

8.3. During Employment

The System Administration and Institutions must require and confirm that all faculty and staff complete annual information security awareness. Faculty and staff shall be provided training for handling sensitive data as appropriate for the employee's role.

8.4. Termination or Changes of Employment

The System Administration and Institutions must have exit procedures in place to ensure the return of all confidential and proprietary information and information resource assets upon termination of employment or written agreement, and ensure

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

8.5. References

8.5.1. 1 Texas Administrative Code §202.77 User Security Practices
8.5.2. ISO 27002 Human Resources Security
8.5.3. Payment Card Industry Data Security Standards 3.0

9. Physical Security

9.1. Purpose

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

9.2. Secure Areas

9.2.1. The System Administration and Institutions must document and manage physical security for mission critical information resources to ensure confidentiality, integrity, and availability of information resources.
9.2.2. All information processing facilities must be protected by physical controls that are appropriate for the size and complexity of the operations and the criticality, sensitivity, regulatory compliance requirements and risks to the systems or services operated at those locations.
9.2.3. Work areas must be protected in accordance with physical controls and security requirements that are appropriate for the type of operational functions performed in the area. The System Administration and Institutions shall develop procedures to distinguish between onsite personnel and visitors in sensitive areas.
9.2.4. Physical security and emergency procedures for information resources must be documented, tested, and reviewed as part of the risk assessment process.

9.3. Equipment Security

9.3.1. Procedures for protecting mission critical information resources from environmental hazards, power failures, and other disruptions must be documented, updated, and tested at least annually.
9.3.2. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

9.3.3. System Administration and Institutions will refer to the State Office of Risk Management for applicable rules and guidelines related to managing physical security.

9.4. References

9.4.1. 1 Texas Administrative Code § 202.73 Managing Physical Security
9.4.2. ISO 27002 Physical and Environmental Security

10. Communications and Operations Management

10.1. Purpose

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

10.2. Operational Procedures and Responsibilities

10.2.1. The principle of least privilege must be established and enforced when developing standards, procedures or assigning access permissions.
10.2.2. A separation of functions must be established for tasks involving information and information resources that are susceptible to fraudulent or other unauthorized activity.
10.2.3. The System Administration and Institutions must follow password policies and procedures that are established by the System Administration or Institution that provides the password management service and that are also consistent with ISO 27002 and 1 TAC 202.75.
10.2.4. The System Administration and Institutions must follow policies and procedures that govern access, management and monitoring of communication networks and devices that are established by the System Administration or Institution that provides the communications service, and that are consistent with ISO 27002 and 1 TAC 202.75.
10.2.5. The System Administration and Institutions must implement controls to protect information and information resources from malicious or unauthorized code. The System Administration or Institution providing the service is responsible for establishing standards for management of anti-virus protection.
10.2.6. The System Administration and Institutions must create procedures for the use of digital signatures that comply with provisions found in 1 TAC §203.

10.3. System Planning and Acceptance

10.3.1. The System Administration and Institutions shall establish policies and procedures ensuring security reviews take place prior to contracting with an external party. The review must meet the requirements of TAC 202.75(6) and include signing of a non-disclosure agreement if confidential data will be used as part of the agreement.

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

10.4. Protection Against Malware, Malicious or Unwanted Programs

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

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

10.4.2. Antivirus software must be kept current.

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

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

10.5. Back-Up

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

10.6. Network Security Management

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

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

10.6.2. Network access must adhere to the principle of least privilege.

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

10.6.4. Networks must be segmented by function.

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

10.6.6. Networks must be monitored.

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

10.7. Media Handling

The System Administration and Institutions must implement policies and procedures regarding the secure management of removable media. Policies should address encryption, storage, transport, and the secure destruction of any data commensurate with the sensitivity or value of the information.

10.8. Exchange of Information

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

10.8.2. Information exchanged with an external institution, agency, or organization must be protected as required by the System Administration or Institution policies in accordance with TAC 202.75(2)(B).

10.9. Electronic Commerce

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

10.10. Monitoring

10.10.1. Monitoring and logging processes shall be established that provide a sufficiently complete history of transactions for auditing purposes and that meet the requirement of 1 TAC §202.75(5).

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

10.10.2.1. Unauthorized use is prohibited;

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

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

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

10.11. References

10.11.1. 1 Texas Administrative Code § 202.75 Information Resources Security Safeguards
10.11.2. 1 Texas Administrative Code Chapter 203 Management of Electronic Transactions and Signed Records
10.11.3. ISO 27002 Communications and Operations Management

11. Access Control

11.1. Purpose

Access to information and information resources must be documented and controlled.

11.2. User Access Management

11.2.1. The System Administration and Institutions shall ensure user access is managed by establishing procedures for granting accounts, managing passwords, regular review of accounts and associated privileges, and reviewing accounts immediately upon change of employment status. Privileges must be limited to the needs of individual users.
11.2.2. User behavior, activities, or the use of computing devices to access institutional networks must not compromise the security of users, information, or information resources.
11.2.3. Institutional or external networks must not be used to compromise the identity of or impersonate individuals or information resources.

11.3. User Responsibilities

11.3.1. Users must be held responsible for all activities that take place using their accounts.
11.3.2. Users must keep their accounts and passwords secure.
11.3.3. Users must keep unattended computing devices secure. This includes automatic password-protected screen savers after a set period of inactivity as well as securing office doors.

11.4. Network Access Control

The System Administration and Institutions shall develop policies that specify who may have access to institutionally owned and managed networks and procedures for provisioning access to the network.

11.5. Operating System Access Control

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

11.5.1. Access to operating systems should be controlled by a secure log on procedure.
11.5.2. All users should have a unique identifier which should be used to trace activities to the responsible individual.
11.5.3. Log on banners specifying a user's rights and responsibilities regarding system usage should be presented to users during the log on process.
11.5.4. Administrator access should be limited to those individuals who have a documented business reason for the access.
11.5.5. Users may not employ tools or utilities capable of overriding system and application controls without permission.
11.5.6. Administrator accounts or accounts with expanded privileges should only be used for administration and management of information resources.
11.5.7. Inactive sessions should be terminated after a defined period of inactivity.

11.6. Application and Information Access Control

11.6.1. The System Administration and Institutions shall develop and implement policies and procedures for granting access to applications and application data.
11.6.2. Access to applications and application data should be restricted according to the principle of least privilege.
11.6.3. Users may not employ tools or utilities capable of overriding application controls.
11.6.4. Access to mission critical applications and Category I application data should be logged or documented by other means.

11.7. Mobile Computing and Teleworking

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

11.8. References

11.8.1. 1 Texas Administrative Code § 202.75 Information Resources Security Safeguards
11.8.2. ISO 27002 Access Control

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

12.1. Purpose

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

12.2. Security Requirements of Information Systems

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

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

12.2.3. The requirements of TAC §202.75(6) must be implemented when testing data or managing test, development, and quality assurance environments.

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

12.3. Correct Processing in Applications

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

12.4. Cryptographic Controls

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

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

12.4.1.2. Confidential information stored in a public location that is directly accessible without compensating controls in place must be encrypted.
12.4.1.3. Storing confidential information on portable devices should be discouraged.
12.4.1.4. Confidential information must be encrypted if copied to or stored on a portable computing device, removable media, or non-agency owned computing device.
12.4.1.5. In instances where no technology exists to encrypt a device, compensating electronic controls must be implemented to secure the device.
12.4.1.6. Encryption of a device must be documented and verifiable.
12.4.1.7. Encryption keys must be managed.

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

12.5. Security in Development and Support Processes

The System Administration and institutions must implement policies and procedures requiring that information security, security testing, and audit controls shall be included in all phases of the system development lifecycle or acquisition process.

12.6. Technical Vulnerability Management

12.6.1. The System administration and institutions must implement policies and procedures for vulnerability assessment and management.

12.6.1.1. Vulnerability assessments may only be performed by documented, authorized individuals.
12.6.1.2. Institutions must create policy and procedures for vulnerability management that include acceptable time frames for addressing vulnerabilities and escalation procedures for handling unaddressed vulnerabilities.

12.7. References

12.7.1. 1 Texas Administrative Code § 202.75 Information Resources Security Safeguards
12.7.2. ISO 27002 Information Systems Acquisition, Development, Testing, and Maintenance

13. Information Security Incident Management

13.1. Purpose

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

13.2. Reporting Information Security Events and Weaknesses

13.2.1. The System Administration and Institutions must establish information security incident management procedures that consider all phases of incident handling.
13.2.2. Information security breaches must be investigated promptly and reported to the Information Security Officer.

13.3. Management of Information Security Incidents and Improvements

13.3.1. In accordance with the requirements set forth in 1 TAC §202.76, the Information Security Officer will assess the incident, oversee incident response, assemble incident response teams as necessary, and will coordinate incident handling, remediation and reporting. Custodians and Information Owners must cooperate with incident investigations.
13.3.2. As required by 1 TAC §202.76, information security breaches must be reported to the Department of Information Resources if they propagate to other state systems, result in criminal violations that are required to be reported to law enforcement, or involve the unauthorized disclosure or modification of confidential information.
13.3.3. Confidentiality of incidents and associated activities must be maintained during all phases of incident handling.

13.4. References

13.4.1. 1 Texas Administrative Code §202.76 Security Incidents
13.4.2. ISO 27002 Information Security Incident Management

14. Business Continuity Management

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

Plans must include a business impact analysis, risk assessment, and a disaster recovery plan as required by 1 TAC §202.74. The business impact analysis determines which information resources are critical. Plans must consider information security, should be tested at least annually and shall be updated as frequently as needed.

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

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

14.4. References

14.4.1. 1 Texas Administrative Code § 202.74 Business Continuity Planning
14.4.2. ISO 27002 Business Continuity Management
14.4.3. ISO 22301 Societal Security -- Business Continuity Management Systems -- Requirements

15. Compliance with Legal Requirements

15.1. Purpose

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

15.2. Data Protection Laws

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

15.3. Acknowledgement of Security Responsibilities

All users of information and information resources of the System, System Administration and Institutions, including faculty, staff, students, guests, contractors, consultants, and vendors shall acknowledge and accept their responsibilities for information security.

15.4. Information Systems Audit Considerations

Audit processes should be implemented in a secure manner and as efficiently as possible while minimizing any disruption to business.

15.5. References

15.5.1. ISO 27002 Compliance with Legal Requirements

16. Security Exceptions

The System Administration and Institutions shall implement procedures for granting and documenting security exceptions in accordance with TAC § 202.75 and § 202.71(c)(1)(H) and (d)(5). The Information Security Officer with the approval of the institution of higher education head or his or her designated representative may issue exceptions to information security requirements or controls. The Information Security Officer will coordinate exceptions and compensating controls with information and service owners. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

17. Sanctions for Violations

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