UNT | SYSTEM
IT Shared Services

Compliance Requirements for Information Technology Systems and Services

Compliance Statement

Information technology systems provisioned for the use, support, or delivery of services to or by UNT System and its Institutions are required to adhere to applicable laws, standards, and policies associated with information resources. Applicable standards include but are not limited to: Information security and accessibility.

Information security practices are largely based in part on standards administered by the State of Texas, however other international, federal, and industry best practice requirements must be met in order to comply with governing authorities and bodies of knowledge.

Information technology systems that are owned and managed by UNT System or institutions must adhere to the requirements noted in in this document. Services, systems, information, and information technology whose use, access, management, processing, or implementation are outsourced to external service providers or vendors must also adhere to these requirements.

Application

In general, all information technology systems must comply with a core body of security requirements as noted in Section 1, “General Security Controls for All Systems and Services”.

Systems or services that require the use of confidential information as part of functionality, must adhere to applicable controls established for protecting data, as noted in Section 2, “Controls for Services and Systems that use Confidential Information”.

Server configuration requirements can be found in Section 3, “Controls for Servers and Other Systems”.

Requirements for applications built by vendors and those developed in-house can be found in section 4, “Controls for Applications”.

Web based services must comply with controls established for secure development and lifecycle management of websites, web applications, and mobile applications, as noted in Sections 5-6, “Controls for Websites and Web Applications”, and “Controls for Mobile Applications”.

Service providers and vendors must comply with controls established in Section 7, “Requirements for Establishing and Maintaining Relationships with Vendors and Service Providers” and Section 8, “Compliance Requirements for Third-Party Vendors of Systems and

Services." Requirements include establishing procedures for ensuring that security aspects of the relationship between UNT System or Institutions are established, documentation expectations when initiating relationships, service delivery management, and changes associated with services.

Exceptions to the application of these controls should be directed to the Chief Information Security Officer for UNT System for approval.

1. General Security Controls for All Systems and Services

a. UNT System Information Security Policy 8.1000 http://www.untsystem.edu/pdfs/policies-admin/08.100/08.100_Information-Security-%2800127965xC146B%29.pdf

b. UNT System Information Security Handbook https://itss.untsystem.edu/sites/default/files/unt_system_information_security_handbook_2016.pdf

c. Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C for Higher Education http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202

d. NIST 800-53 revision 4 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

e. International Organization for Standardization Information Technology- Security Techniques- Code of Practice for Information Security management (ISO 27002)

f. SANS Critical Security Controls https://www.sans.org/critical-security-controls/

2. Controls for Services and Systems that Use Confidential Information

a. See *General Security Controls for All Systems and Services*

b. Confidential information is defined as 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.

c. Confidential information must be encrypted when transmitted over a public network; when stored in a public location that is accessible without compensating controls in place; and when copied to, or stored on, a portable computing device, removable media, or a non-state organization owned computing device.

d. Approval to use confidential information in an information system or service must be obtained from the respective information owner. See the IT Shared Services website for more information, http://informationowners.untsystem.edu/

e. Family Educational Rights and Privacy Act (FERPA, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

f. Health Insurance Portability and Accountability Act (HIPAA, http://www.hhs.gov/ocr/privacy/)

g. Payment Card Industry Data Security Standards (PCI-DSS, https://www.pcisecuritystandards.org/security_standards)

h. Gramm-Leach-Bliley Act (GLBA, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)

i. UNT System Non-Disclosure Agreement (contact CISO for UNT System)

3. Controls for Servers and Other Systems

a. See *General Security Controls for All Systems and Services*

b. See *Controls for Servers and Systems that Use Confidential Information*

c. SANS Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers https://www.sans.org/critical-security-controls/control/3

d. Center for Internet Security (CIS) Benchmark Division Resources, https://benchmarks.cisecurity.org/downloads/multiform/index.cfm. Use the latest versions of CIS Security Benchmarks for Windows, Windows Server, Apple OSX, and Red Hat Enterprise. As of the date of this document, the following are applicable:

   i. CIS Microsoft Windows 7 Benchmark v2.1.0

   ii. CIS Microsoft Windows Server 2008 R2 Benchmark v2.1.0

   iii. CIS Apple OSX 10.10 Benchmark v1.0.0

   iv. CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0

e. Secure server design and configuration must be included in all phases of development and implementation. Web servers must not be susceptible to security vulnerabilities, including those found in the OWASP Top 10 Security Risks, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

f. Cryptographic Key Management Requirements

   v. Encryption must be employed to ensure secure transmission of confidential information, e.g., SSL.

   vi. The minimum length strength for protecting confidential information is 128-bit encryption algorithm.

   vii. Encryption keys must be managed using automated mechanisms with supporting procedures or manual procedures. Encryption keys must be secured.

4. Controls for Applications

a. See *General Security Controls for All Systems and Applications*

b. See *Controls for Servers and Systems that Use Confidential Information*

c. SANS Critical Security Control No. 6, Application Software Security, https://www.sans.org/critical-security-controls/control/6

5. Controls for Web Applications and Web Sites

a. See *General Security Controls for All Systems and Services*

b. See *Controls for Servers and Systems that Use Confidential Information*

c. UNT System Web Hosting Policy, https://itss.untsystem.edu/cws/web-hosting-policy

d. State Websites, Texas Administrative Code, Title 1, Part 10, Chapter 206(C) - see https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=206&sch=C&rl=Y

e. Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), http://www.section508.gov/content/learn/laws-and-policies

f. Secure website design and configuration must be included in all phases of development and implementation. Website must not be susceptible to security vulnerabilities, including those found in the OWASP Top 10 Security Risks, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

g. Compatibility with web browsers/versions supported by the UNT System

h. Websites must be compatible with mobile devices

6. Controls for Mobile Applications

a. See *General Security Controls for All Systems and Services*

b. See *Controls for Servers and Systems that Use Confidential Information*

c. SANS Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers https://www.sans.org/critical-security-controls/control/3

d. OWASP Top 10 Mobile Controls and Design Principles https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Controls

e. OWASP Mobile Application Coding Guidelines https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Secure_Mobile_Development

7. Requirements for Establishing and Maintaining Relationships with Vendors and Service Providers

a. UNT System Information Security Handbook, Section 15, V Relationships, UNT System Information Security Handbook. https://itss.untsystem.edu/sites/default/files/unt_system_information_security_handbook_2016.pdf

8. Compliance Requirements for Third-Party Vendors of Systems and Services

a. Adhere to UNT System IT Compliance Requirements for Information Technology Systems and Services (Requirements of this Document and 1 TAC § 202.72(2)(A)).

b. Implement remedial information security actions to adequately address non-compliance issues or risks identified during the UNT System review of the System Acquisition Survey and throughout the system development lifecycle (1 TAC § 202.76 and State of Texas Security Controls Standards Catalog PM-4).

c. Agree to adhere to Vendor Requirements found in Section 15 of the UNT System Information Security Handbook.

d. Report data breaches to information security immediately upon discovery and provide evidence of remediation (1 TAC 202.72(2)(C), 1 TAC 202.74(1) and (2), UNT System Incident Reporting, and UNT System Information Security Handbook Section 16.2.2).

e. Provide evidence that information/data stored in third-party systems is recoverable and contingency plans are in place (1 TAC 202.72(2), 1 TAC 202.76: Security Controls Standards Catalog CP 2-11, and 1 TAC 202.76: Security Controls Standards Catalog CP 2-11).

f. Adhere to the network connections policy, which limits/restricts the types of devices that are allowed to connect to the institutional networks (1 TAC 202.72(2)(A), UNT System Information Security Handbook, and UNT Network Connections Policy).

g. Conduct website and mobile application vulnerability and penetration testing prior to deployment (Texas Government Code § 2054.517).

h. Submit architectural designs of applications, information systems, and websites; and submit network/system diagrams of information systems (Texas Government Code § 2054.517, 1 TAC 202.76: Security Controls Standards Catalog SC-7, and 1 TAC 202.76: Security Controls Standards Catalog PL-8).

i. Provide authentication mechanisms for information systems and applications (Texas Government Code § 2054.517).

j. Provide administrator access levels to data that will be processed within information systems (Texas Government Code § 2054.517).

k. Provide data flow diagrams representing the flow of a data within an information system (1 TAC 202.76: Security Controls Standards Catalog AC-4, PL-8, and SC-7).

l. Provide evidence of the remediation of electronic and information resources accessibility deficiencies and gaps (1 TAC 213.38(b)(1-2), 1 TAC 213.38(d), and 1 TAC 206.70(a), (c), (f))

m. Ensure that information systems are designed and configured to adhere to State of Texas requirements for secure architectural design (Enterprise architecture designs will be provided upon initiation of agreement with third-party), (1 TAC § 202.72(2)(A-E), 1 TAC 202.76: Security Controls Standards Catalog SA-17, and 1 TAC 202.76: Security Controls Standards Catalog PL-2).

n. Provide reports on security performance (1 TAC 202.76: Security Controls Standards Catalog PM-6-7 and UNT System Information Security Handbook 15.4).

o. Require third-party personnel that will access institutional information or information systems to complete institutionally offered information security awareness training or provide evidence of training offered through organization prior to accessing institutional information or information resources (1 TAC 202.76: Security Controls Standards Catalog AT-2 and AR-5).

Contact Information

Office of the Chief Information Security Officer
IT Shared Services, UNT System
security@untsystem.edu
940-369-7800

Document Version Log

Version	Approved By	Date	Description
1	Charlotte Russell	06/04/2014	
2	Charlotte Russell	09/16/2016	
3	Pamela Johnson	08/27/2019	Incorporated compliance requirements for third-party vendors of systems and services.