Compliance Requirements for Information Technology Systems and Services

Compliance Statement

Information technology systems that are 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 security practices. These 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.

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".

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.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. Family Educational Rights and Privacy Act (FERPA, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
e. Health Insurance Portability and Accountability Act (HIPAA, http://www.hhs.gov/ocr/privacy/)
f. Payment Card Industry Data Security Standards (PCI-DSS, https://www.pcisecuritystandards.org/security_standards)
g. Gramm-Leach-Bliley Act (GLBA, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)
h. 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
   i. Encryption must be employed to ensure secure transmission of confidential information, e.g., SSL.
   ii. The minimum length strength for protecting confidential information is 128-bit encryption algorithm.
   iii. 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*
a. See *Controls for Servers and Systems that Use Confidential Information*
b. 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

b. See *General Security Controls for All Systems and Services*
c. See *Controls for Servers and Systems that Use Confidential Information*
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