Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2018
Policy 5.8.8	**Information Resource Security Configuration Management**	Responsibility:	Chief Information Security Officer

INFORMATION RESOURCE SECURITY CONFIGURATION MANAGEMENT

Policy

The Chief Information Security Officer (CISO) shall establish and communicate security "hardened" configuration standards that incorporate procedures for managing system platforms that minimize vulnerability, protects against threats and complies with UT Health San Antonio policies and state and federal laws for all Information Resources owned, leased or under the control of the University. All security configuration standards must minimally specify:

a. Information Resource Custodians shall implement baseline security configurations and maintenance protocols (such as security checklists) for securing the particular system platform(s) under their control. Reference "Security Configuration Baselines" for current operating system, platform and software configuration standards;

b. Information Resource Custodians shall ensure that vendor supplied patches are routinely acquired, systematically tested prior to implementation where practical, and installed promptly based on risk;

c. Information Resource Custodians shall remove unnecessary software, system services and drives;

d. Information Resource Custodians shall enable security features included in vendor-supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections and other file protections;

e. Information Resource Custodians shall disable or change the password of default accounts before placing the resource on the UT Health San Antonio network;

f. Mission Critical Information Resources and information resources that store or process sensitive data shall be configured to enable logging of access and operating system activity. Access to logs

and monitoring data shall be restricted to the CISO and explicitly authorized by the CISO;

g. Information Resources shall be configured to report its hardware and software configuration state to a centralized tracking system designated and maintained by the CISO;

h. Information Resource Custodians shall provide the CISO with timely information on the security configuration and operating state for information resources under their control;

i. Information Resource Custodians shall ensure access management controls are enabled to meet UT Health San Antonio policies and standards including, but not limited to, registration to the UT Health San Antonio active directory domain and use of two-factor authentication for remote access;

j. access rights shall be granted by the Information Resource Custodian and Owners when requested by the CISO to execute security incident response, containment ad discovery actions;

k. access privileges shall be set utilizing the least privileged principle of providing the minimum amount of user, application and process access required to execute essential functions;

l. privileged or special access to operating systems shall be based on essential need and approved by the CISO. Accounts entitled with privileged or special access shall be unique and separate from a user's standard account (account not entitled with special or privileged access rights);

m. Information Resources shall be configured to encrypt data-at-rest and in-transit in compliance with UT Health San Antonio policies and standards;

n. Information Resources shall be tested in accordance with policies and standards set by the CISO for known vulnerabilities periodically or when new vulnerabilities are announced;

o. Information Resources shall be configured to grant the CISO with direct access to detailed security status information including, but

not restricted to, firewall rules, IPS/IDSs rules, security configurations and patch status; and sufficient access rights to independently perform traffic and log monitoring, asset tracking and classification, configuration monitoring and testing and vulnerability scanning;

p. software must be installed and operated in accordance with the applicable licensing agreement. Unauthorized or unlicensed use of software is prohibited; and

q. Information Resources with an operating system that is no longer supported by its vendor may not be connected to the UT Health San Antonio network.

i. Vendor support requires:

- timely issuance of security patches to mitigate vulnerabilities identified in the operating system; or
- the operating system is not designated as "End-of-Life" and "End-of-Support" by its vendor.

The CISO shall ensure that devices are administered by professionally trained staff in accordance with UT Health San Antonio's policies, standards and procedures.

Smartphones, tablets and any device utilizing an operating system explicitly developed for mobile computing devices are exempt from this policy and must comply with Section 5.8.12, "Mobile Device and Personally Owned Computing Policy" in the *Handbook of Operating Procedures* (HOP).

Network Security

The Infrastructure and Security Engineering (ISE) Department of Information Management and Services (IMS) is designated as the Information Resource Owner and exclusively responsible for the UT Health San Antonio Network Infrastructure including, but not limited to, the local area network, data center infrastructure, wide area and telecommunications networks, Internet, OTS network and wireless/Wi-Fi networks.

a. All network devices connecting to the UT Health San Antonio Network Infrastructure will be security hardened based on risk.

b. The network infrastructure shall be segmented either physically or logically to reduce the scope of exposure of information resources commensurate with the risk.

c. Configuration changes of network devices require approval of ISE and must be performed in compliance with Section 5.8.24, "Change Management Security Policy" in the HOP.

d. No hardware device or software that provides network services shall be installed within or connecting to the UT Health San Antonio Network Infrastructure without ISE approval.

    i. All connections of the network infrastructure to external or third party networks (including Internet, telecommunications and business partner networks) must be approved by ISE.

    ii. No extension or retransmission of computer network services by installation of a router, switch, hub, wireless access point or controller, cellular signal booster, dual ported computer or software application is permitted unless approved by ISE.

e. No hardware device or software that scans the UT Health San Antonio network, computing devices or external networks for device configuration and operating state (including software or hardware that attempts to exploit vulnerable device configurations) shall be installed or executed without the explicit approval by the CISO.

f. All firewalls and network security devices must be installed and maintained by ISE unless explicitly permitted by the CISO.

g. Networking addresses for supported protocols are allocated, registered and managed by ISE.

i. Network directory services and network address space services (including, but not limited to, DNS and DHCP services) shall be exclusively provided and managed by ISE.

ii. Any information resource use of non-sanctioned protocols must be approved by ISE.

h. ISE may disable or restrict access to devices or network segments that demonstrate suspicious or abnormal behavior or deemed vulnerable to attacks or breach.

Server and Storage Device Security

All computing and storage devices that provide access to or host centralized resources, services or applications to other computers on the UT Health San Antonio network infrastructure or external networks must be maintained in a manner that provides physical and logical security commensurate with risk.

a. All servers, regardless of administration responsibility, must be located in a data center owned, leased or otherwise controlled by Information and Management Services (IMS).

i. Connectivity to servers and storage devices discovered outside of an approved data center shall be restricted.

ii. Exceptions must be approved by the Vice President and Chief Information Officer.

b. Storage devices that source data to centralized resources, services or applications or services to other computers on the UT Health San Antonio network infrastructure or external networks must be located in a data center owned, leased or otherwise controlled by IMS. Exceptions are allowed in the following circumstances:

i. storage connected to scientific or medical instruments/devices. Appropriate Physical and Security Access Control Standards and Practices commensurate

with the risk of the data stored on these devices must be applied and the Chief Information Security Officer shall maintain documentation of these devices; and

ii. external storage devices used for local computer backup/archive. These storage devices must be encrypted per UT Health San Antonio policies and standards.

c. Servers and data shall be segmented either physically or logically to reduce the scope of exposure commensurate with risk.

i. Production servers and data must be segmented from test and development environments.

ii. Internet accessible applications and data must be segmented from internal applications and databases.

iii. Confidential data should not be stored on the same server or storage device as non-sensitive data.

- If both data types must be stored on the same server or storage device, compensating controls must be implemented to protect unauthorized access or disclosure of confidential data.

d. Servers with an operating system that is no longer supported by its vendor may not be connected to the UT Health San Antonio network.

i. Vendor support requires:

- timely issuance of security patches to mitigate vulnerabilities; or

- the operating system is not designated as “End-of-Life” and “End-of-Support” by its vendor.

ii. An exception may be granted to allow limited access to the server (e.g., access to internal UT Health San Antonio networks or devices only) if upgrading the operating system to a supported version or alternate platform adversely impacts its required use or function.

References

- U.T. System Policy 165 Standard 19
- U.T. System Policy 165 Standard 20