Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.8	**Information Resource Security Configuration and Management**	Responsibility:	Chief Information Security Officer

INFORMATION RESOURCE SECURITY CONFIGURATION AND MANAGEMENT

Policy

UT Health San Antonio shall adopt and document Standards and Procedures to define and manage a secured operating configuration for all Information Resources owned, leased or under the control of the University. Security objectives shall include:

a. hardware standards to ensure consistency in the platforms supported by UT Health San Antonio;

b. a lifecycle framework to define the implementation, testing, availability, support and disposal of the Information Resource;

c. security configuration (hardening) standards that address vulnerabilities, minimize risk and comply with all UT Health San Antonio policies;

d. monitoring standards to ensure compliance with UT Health San Antonio Policies and Standards and protection against vulnerabilities; and

e. standards for patch management and vendor support of application and operating system environment.

The Chief Information Security Officer shall ensure that Information Resources are administered by professionally trained staff in accordance with UT Health San Antonio Policies, Standards and Procedures.

All Owners and Custodians of UT Health San Antonio owned, leased, or controlled Information Resources must provide the Chief Information Security Officer with direct access to detailed security status including, but not restricted to the following:

- firewall rules;
- IPS/IDS rules;

- security configurations and patch status; and
- sufficient access rights to servers and computing devices to independently perform traffic and event monitoring and log analysis.

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, 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 *Handbook of Operating Procedures* (HOP), Standards and Procedures.

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. All firewalls and network security devices must be installed and maintained by ISE unless explicitly permitted by the Chief Information Security Officer.

f. 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 provided and managed by ISE.

   ii. Any Information Resource use of non-sanctioned protocols must be approved by ISE.

g. ISE shall adopt Standards and Procedures for:

   i. configuring and managing baseline security hardened standards for all network devices;

   ii. defining networking protocol standards, segmentation architecture and address schemes/ranges;

   iii. administration of network directory and address space services;

   iv. managing access to the Network Infrastructure in accordance with Information Security Policies and Standards.

   v. testing and installing security updates and service packs to operating systems and applications for network devices;

   vi. monitoring network activity traversing a network device and the Network Infrastructure;

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

vii. maintaining a list of authorized Networking Devices that connect to the UT Health San Antonio Network Infrastructure and associated connectivity and traffic flow diagrams; and

viii. identifying and assigning appropriately trained administrators for all network devices.

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 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. Software installed on servers and storage devices is to be used in accordance with the applicable licensing agreement. Unauthorized or unlicensed use of software is prohibited.

e. 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.

f. All servers connecting to the UT Health San Antonio Network (including, but not limited to, the internal network, external or perimeter networks and business partner networks) will be security hardened based on risk. Minimum configuration Standards shall include:

   i. registration to the UT Health San Antonio Active Directory Domain;

   ii. encryption in compliance with UT Health San Antonio Policies, Standards and Procedures;

   iii. timely installation of security patches for the Operating System and application software installed on the server;

   iv. active and up-to-date anti-malware software in compliance with UT Health San Antonio Policies, Standards and Procedures;

   v. logging of access and Operating System functions; and

   vi. Reporting of its hardware and software configuration state to a centralized repository.

g. To ensure patch management, vulnerability prevention updates and reporting of authorized computing assets. IMS shall:

   i. define baseline security hardened configuration Standards for all servers;

   ii. maintain documentation of authorized servers and their hardware and software configuration status including servers with operating systems that cannot connect to the UT Health San Antonio Active Directory Domain;

iii. facilitate testing and timely installation of service packs, hot fixes and security patches; and

iv. identify and assign appropriately trained administrators.

Computer Device Security

Computing devices (including, but not limited to, workstations and laptops, regardless of operating systems) connecting to the UT Health San Antonio network or used to create, store or transmit Data must be maintained in a manner that provides physical and logical security commensurate with risk.

a. 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 HOP.

b. All computing devices will be security hardened based on risk. Minimum configuration standards shall include:

i. registration to the UT Health San Antonio Active Directory Domain;

ii. encryption in compliance with UT Health San Antonio Policies, Standards and Procedures;

iii. timely installation of security patches for the Operating System and application software installed on the computing device;

iv. active and up-to-date anti-malware software in compliance with UT Health San Antonio Policies, Standards and Procedures;

v. storage of confidential and mission critical data to servers or centrally managed storage devices;

- if confidential and/or mission critical data must be

stored on a computing device, the device shall be configured to regularly archive the data to a separate or external storage device.

vi. logging of access and Operating System functions; and

vii. reporting of its hardware and software configuration state to a centralized repository.

c. Access to computing devices shall be granted in compliance with UT Health San Antonio Policies and Standards.

- Use of Administrator or other privileged accounts shall be limited to only required functions and segregated from a standard user accounts.

d. Software installed on computing devices is to be used in accordance with the applicable licensing agreement. Unauthorized or unlicensed use of software is prohibited.

e. Computing devices 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.

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.

f. Information Management and Services (IMS) shall maintain a central repository of hardware and software security status for each computing device.

References

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