The Division of Information Technology
University Information Security Standards

Information Security Standard – Network Configuration (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

The information resources network infrastructure is provided by West Texas A&M University for University departments. It is important that the infrastructure, which includes media, active electronics and supporting software, be able to meet current performance requirements, while retaining the flexibility to allow emerging developments in high-speed networking technology and enhanced user services.

2. Applicability

This information security standard applies to all University network infrastructure information resources.

The purpose of this information security standard is to provide a set of measures that will mitigate information security risks associated with network configuration. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The purpose of the West Texas A&M University Network Configuration Security Policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of West Texas A&M University information.

The intended audience is all network system administrators of university information resources.

3. Definitions

3.1 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.2 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.3 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

3.4 User: An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

4. Procedures

4.1 Information Technology is responsible for the university network infrastructure configuration and will continue to manage further developments and enhancements to this infrastructure.

4.2 All new or upgraded cabling will conform to state standards for cabling (Texas Administrative Code Chapter 208) to the extent consistent with the university's mission.

4.3 All departments shall consult with Network Services for allocation and registration of network addresses, name space, and other configuration changes. Network Services must approve such configurations and assignments.

4.4 All network connected equipment must be configured to a specification approved by West Texas A&M University information technology – network services.

4.5 All hardware connected to the West Texas A&M University network is subject to West Texas A&M University information technology management and monitoring standards.

4.6 Changes to the configuration of active network management devices must not be made without the approval of West Texas A&M University information technology – network services or the IRM.

4.7 The West Texas A&M University network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned and/or approved protocols must be approved by West Texas A&M University information technology – network services.

4.8 The networking addresses for the supported protocols are allocated, registered and managed centrally by West Texas A&M University information technology – network services.

4.9 All connections of the network infrastructure to external third party networks, including Internet Service Providers, is the responsibility of information technology – network services. This also includes connections to external telephone networks.

4.10 West Texas A&M University information technology firewalls must be installed and configured following the West Texas A&M University firewall implementation standard documentation.

4.11 The use of departmental firewalls is not permitted without the written

authorization from the West Texas A&M University Information Resources Manager (IRM).

4.12 Users must not extend or re-transmit network services in any way. This means that you must not install a router, switch, hub, or wireless access point to the West Texas A&M University network without the approval of the West Texas A&M University Information Resources Manager (IRM).

4.13 Users must not install network hardware or software that provides network services without the approval of the West Texas A&M University Information Resources Manager (IRM).

4.14 Users are not permitted to alter network hardware in any way.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer