The Division of Information Technology
University Information Security Standards

Information Security Standard – Network Access (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 all University departments. It is important that the infrastructure, which includes media, active electronic equipment (i.e., routers, switches, cables, etc.) 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 standard applies to all university network information resources.

The purpose of this standard is to provide a set of measures that will mitigate information security risks associated with Network Access. 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 West Texas A&M University Network Access Policy applies equally to all individuals with access to any West Texas A&M University Information Resource.

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 Users are permitted to use only those network addresses issued to them by West Texas A&M University.

4.2 Users are not permitted to extend or re-transmit network services, including wireless, in any way. Network aggregation devices (e.g. hubs, switches, routers) shall not be connected to the network infrastructure

without prior approval by the West Texas A&M University Information Resources Manager (IRM).

4.3 Network management/control devices shall not be connected to network infrastructure without prior consultation with the IT Division's Network Services department.

4.4 Management of network addresses and name space is managed by Network Services. Users are permitted to use only those network addresses issued to them by Network Services.

4.5 End-users are not to connect to or install any equipment to the network infrastructure without prior approval from Network Services. Additionally, end-users shall not alter or disable University network infrastructure devices or equipment.

4.6 Granting anonymous access to the network is not permitted. Unauthorized wireless networks are strictly prohibited.

4.7 Network scans and network vulnerability scans of devices attached to the West Texas A&M University network as well as the appropriate remediation are occasionally necessary to ensure the integrity of West Texas A&M University computing systems. Network scans and network vulnerability scans may only be conducted by university employees designated by the information technology network manager, information security officer (ISO), or the information resources manager (IRM).

4.8 Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a systems. For example, West Texas A&M University users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the West Texas A&M University network infrastructure.

4.9 Users are not permitted to alter network hardware in any way shape for form.

4.10 Management of West Texas A&M University network addresses, address space, and network naming will be managed by information technology. Users are permitted to use only those network addresses issued to them by information technology.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer