The Division of Information Technology
University Information Security Standards

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

1. General

Firewalls not only prevent unauthorized access to or from a private network, but are a fundamental element of West Texas A&M University's information systems security infrastructure. Firewalls regulate and control Internet connectivity and necessary Internet services such as web browsing, mail services, and file transfers. Firewalls establish a perimeter where access controls are enforced.

2. Applicability

This standard applies to University information resources that store, process, or transmit mission critical and/or confidential information.

The purpose of this standard is to provide a set of measures that will mitigate information security risks associated with Internet connectivity. 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 are to be determined by the department heads and their identified information security administrators in accordance with Texas Administrative Code 202 - Information Security Standards.

The intended audience for this standard administrative procedure includes, but is not limited to, all information resources management personnel, owners, and system administrators.

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.

3.2 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.

3.3 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.

3.4 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.

3.5 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

3.6 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

4. Procedures

4.1 All university Internet access will be consolidated and provided through the division of information technology. Individual divisions, departments, and/or colleges will not be permitted to establish independent Internet

connectivity outside of the centralized information technology infrastructure, which also includes off campus departments such as the SBDC, and the Enterprise Network. All requests for Internet access will be directed to the division of Information Technology and approved by the Information Resources Manager/Chief Information Officer.

4.2 The information technology – network services manager is immediately responsible for the monitoring and configuration of all firewall rule sets. The information security officer (ISO) is responsible for enforcing all applicable firewall policies. The information security officer (ISO) shall also coordinate with the State of Texas Department of Information Resources (DIR) to coordinate annual controlled penetration testing and web application vulnerability assessments.

4.3 All university perimeter firewalls shall be independent hardware appliances that provide a separate and unique layered architecture. The use of virtual firewalls or firewall blades within the private and secure core infrastructure is not permitted.

4.4 All West Texas A&M University firewalls must be located in a locked room accessible only to those who must have physical access to such firewalls to perform the tasks associated with firewall management. The placement of firewalls in open and unsecured areas is strictly prohibited. All physical security policies shall be enforced in regards to firewalls.

4.5 The university perimeter firewall permits the following inbound and outbound Internet traffic:

4.5.1 Allow all outbound or egress traffic to Internet services outside of the university with the exception of network traffic that violates university policy, state, and/or federal laws. Network traffic that contains unauthorized services, viruses, worms, or other malware may be blocked by information technology – network services at any time to protect the integrity and reputation of West Texas A&M University. Software as a Service residing in the cloud may also be blocked by risk management decisions.

4.5.2 Allow all inbound or ingress traffic from outside of the university that supports the mission of West Texas A&M University. A complete list of all ingress protocols, applications, and ports that are permitted through the perimeter firewall are maintained by the information security officer (ISO) and the manager of information technology - network services.

4.6 Alarm and alert functions as well as audit logging of any and all firewalls and/or other network perimeter access control systems shall be enabled.

4.7 All firewall activity must be monitored and logged by information technology – network services. Such logs may contain suspicious activity, which might be in indication of unauthorized usage or access attempts to

compromise established security measures. Additional logging devices and/or other third party inspection appliances shall be used to provide further analysis into network traffic crossing the boundaries of the university's Internet borders. The retention of such logs will follow the same retention policy set forth in the backup policy.

4.8 Auditing and testing to verify the firewall's configuration, rule set accuracy, and effectiveness shall be conducted on an annual basis by the State of Texas Department of Information Resources (DIR). Such testing shall include a controlled penetration test of all public network address space used by the university. Remote offices will also be scanned during this annual process. Web application vulnerability assessments will also be conducted on public facing web application servers. Formal reports generated from these tests will be delivered to the university's information resources manager (IRM) and corrections will be made by the information technology – network services manager and the information security officer (ISO).

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer