29.01.03.H0.09 Firewall

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

Texas A&M University-Texarkana (TAMUT) is protected by a firewall in order to restrict Internet access from the campus network to authorized connections only. A firewall is a computer system which is designed to block unauthorized access and allow only predefined criteria of communications.

Reason for Procedure

This document describes the requirements for mitigating network connection risks with the use of a firewall. It must be used as a guide to assess potential risks of applications and their connections to and from the Internet. It also defines the procedures for amending the rules of the firewall. This procedure applies to all individuals who use TAMUT Information Resources.

Definitions

DMZ (Demilitarized Zone): An area, a physical or logical subnetwork where external facing services reside and are accessible to an untrusted network such as the Internet. Also known as a perimeter network.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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.

Information Resources Manager (IRM): Person responsible to the State of Texas for management of the agency’s information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the 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. At TAMUT, the IRM is the CIO.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMUT’s internal and external point of contact for all information security matters.

Intrusion detection system (IDS): A system or software that monitors activities of networks or systems for malicious activities or policy violations capable of producing reports of such information.

Procedures and Responsibilities

1. GUIDANCE AND DIRECTION

The ISO will provide guidance and direction in the following areas:

1.1 Firewall architecture

1.2 Protocols and applications that are permitted through the firewall, both inbound and outbound

1.3 Traffic monitoring rule set

1.4 Approval process for updating or changing rule sets

1.5 Auditing and testing to verify a firewall’s configuration, rule set accuracy, and effectiveness

2. PHYSICAL ARCHITECTURE

2.1 TAMUT Internet access is consolidated and provided by the Information Technology Department.

3. FIREWALL PORT OPENINGS

3.1 TAMUT’s firewall blocks all ports and protocols by default, except for authorized network traffic according to the firewall access list.

3.2 Requests to amend the access list must be approved by the ISO after careful consideration based on the security risk.

3.3 Any traffic that has the potential to cause loss of data integrity, confidentiality, or network availability will immediately be blocked on the firewall perimeter list. A Firewall Perimeter Exception Request form must still be submitted.

3.4 Not all ports are allowed to open on TAMUT’s firewall.

4. TRAFFIC MONITORING AND RULE ENFORCEMENT

4.1 All firewall activity must be monitored and logged.

4.2 Traffic monitoring is the responsibility of the information technology team.

4.3 The ISO is responsible for enforcing firewall/DMZ/IDS rules.

5. AUDITING AND TESTING

5.1 The State of Texas Department of Information Resources (DIR) will conduct annual controlled penetration tests to verify the firewall's configuration.

5.2 Findings of the controlled penetration test will be delivered to the IRM, and corrections will be enforced by the ISO.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publication

Contact Office

Information Security Officer
903-886-5425