PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.24 Information Resources - Firewalls
Approved September 4, 2013
Revised December 7, 2018
Next Scheduled Review: December 2023

UAP Purpose

This purpose of this University Administrative Procedure (UAP) is to provide users of Prairie View A&M University (PVAMU) information resources with information on where to find expert guidance for administering both host-based and departmental firewalls. A firewall is the first line of defense against unauthorized or malicious access to PVAMU information resources. It is of significant importance to ensure that firewalls protecting University information resources are correctly configured. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager (IRM) – person responsible to the State of Texas for management of the University's information resources. The designation of an IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the University's information activities, and ensure greater visibility of such activities within the University. 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 University. If an IRM is not designated, the title defaults to the University's executive director who then will be responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO) - person responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

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.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Firewall - a software or hardware device or system that filters communications between networks that have different security domains based on a defined set of rules. A firewall may be configured to deny, permit, encrypt, decrypt or serve as an intermediary (proxy) for network traffic.

Host-based Firewall - software that functions on a single host (i.e., a single computer including laptop computers) that can permit or deny incoming or outgoing traffic to or from only that host (as opposed to a network-based firewall which protects one or more networks of hosts).

Official Procedures and Responsibilities

---

1. GENERAL

1.1 Firewalls not only prevent unauthorized access to or from a private network, but are a fundamental element of PVAMU'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

2.1 This UAP applies to all firewalls owned, rented, leased or otherwise controlled by PVAMU network users. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

3. RESPONSIBILITIES

3.1 All PVAMU internet access will be consolidated and provided through the Office of Information Technology Services (ITS). Individual divisions, departments, and/or colleges will not be permitted to establish independent internet connectivity outside of the centralized information technology infrastructure. All requests for internet access will be directed to ITS and approved by the Information Resources Manager/Chief Information Officer.

3.2 ITS is 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 ISO shall also coordinate with the State of Texas Department of Information Resources (DIR) to conduct annual vulnerability assessments.

3.3 All PVAMU perimeter firewalls shall be independent hardware appliances that provide a separate and unique layered architecture.

3.4 All PVAMU perimeter 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 perimeter firewalls in

open and unsecured areas is strictly prohibited. All physical security policies shall be enforced in regards to firewalls.

3.5 The University perimeter firewall permits the following inbound and outbound internet traffic:

3.5.1 Allow all outbound or egress traffic to internet services outside of the University with the exception of network traffic that violates University procedures, state, and/or federal laws. Network traffic that contains unauthorized services, viruses, worms, or other malware may be blocked by ITS at any time to protect the integrity and reputation of PVAMU; and,

3.5.2 Allow all inbound or ingress traffic from outside of the University that supports the mission of PVAMU. A complete list of all ingress protocols, applications, and ports that are permitted through the perimeter firewall are maintained by the ISO and ITS.

3.6 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.

3.7 All firewall activity must be monitored and logged by ITS. Such logs may contain suspicious activity, which might be an 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 be maintained by the ISO as per the Record's Retention Schedule.

3.8 Auditing and testing to verify the firewall's configuration, rule set accuracy, and effectiveness shall be conducted on an annual basis by the ISO. Such testing may 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 related departments and monitored by the ISO.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Contact Office

Office of Information Resources Management	936-261-9350