PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.27 Information Resources – Vulnerability Assessments
Approved May 3, 2013
Revised June 11, 2018
Next Scheduled Review: June 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to mitigate the risks that vulnerabilities may pose to Prairie View A&M University (PVAMU) information resource systems. This UAP seeks to ensure that vulnerabilities are adequately addressed and minimized; and, that guidelines are in place to restrict network scanning activity except in limited circumstances. Additionally, all operating systems for all information resource systems must undergo a regular vulnerability assessment as required by Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

To ensure that vulnerability assessments for PVAMU information resources are conducted, the Information Security Officer (ISO) may scan any device or endpoint attached to the University network system at any time.

Definitions

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.

Network Scanning - the process of transmitting data through a network to elicit responses in order to determine the configuration state of an information system.

Network Vulnerability Assessments - assessing network scanning data to determine the presence of security vulnerabilities in the information system.

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.

Official Procedures and Responsibilities

1. APPLICABILITY

1.1 All departments must obtain prior approval from the ISO and Information Technology Services (ITS) before systems can be connected to the network.

Approval must be obtained by completing the Internet Protocol (IP) Address Service Request Form.

1.2 The ISO will monitor vulnerability assessment scans on a quarterly basis.

2. GUIDELINES

2.1 A vulnerability assessment may include assessment(s) of any of the following information resources:

2.1.1 Network(s);

2.1.2 Operating system(s); and,

2.1.3 Application(s).

2.2 An information security assessment will be coordinated by the ISO biennially (every two years) based on a risk analysis developed by the ISO; and, at other times as needed by current threats.

2.3 The ISO is authorized to conduct network scanning of devices attached to the University network. Information gathered from such scans will be used for network management, which includes but not limited to:

2.3.1 Notifying owners of vulnerabilities;

2.3.2 Determining incorrectly configured systems; and,

2.3.3 Validating firewall access requests.

2.4 Custodians of information resources found to be vulnerable in any way will be contacted concerning any identified risk(s). The custodian is responsible for ensuring that the identified risk(s) is mitigated in a timely manner.

2.5 If known vulnerabilities are not resolved, access for the affected information resource(s) will be disabled from the network by the ISO.

2.6 Network scanning may only be conducted with prior approval from the ISO.

2.7 Departments can request vulnerability scans to be conducted on their systems by contacting the ISO.

Related Statutes, Policies, Regulations and Rules

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

Security Control Standards Catalog

System Policy 29.01 Information Resources

System Regulation 29.01.03 Electronic Information Services Access and Security

Contact Office	
Office of Information Resources Management	936-261-9350