PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.12 Information Resources - Security Monitoring

Approved May 26, 2009
Revised September 4, 2013
Revised August 14, 2017
Revised January 19, 2023
Next Scheduled Review: January 1, 2028

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to ensure that effective information resource security controls are in place and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. 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.

Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) - allows departments to register and perform a baseline security risk assessment of their information systems.

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

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.

Official Procedures and Responsibilities

1. GENERAL

1.1 Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as: review of user account logs, application logs, data backup and recovery logs, etc.

1.2 In addition to local monitoring, the Security Operations Center (SOC), part of the Texas A&M University System, will monitor and scan the network and attached devices and stores for security purposes. This is per System Regulation 29.01.03 Information Security.

1.3 In accordance with Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP 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).

2. APPLICABILITY

2.1 This UAP applies to all Prairie View A&M University (PVAMU) managed information resources containing mission critical information, confidential information, and other information resources as may be managed by PVAMU. The intended audience for this UAP includes, but is not limited to, all information resources data/owners, management personnel, and system administrators.

3. PROCEDURES AND RESPONSIBILITIES

3.1 Automated management tools will be utilized by the ISO and Center for Information Technology Excellence (C.I.T.E) to provide real-time notifications and appropriate responses, as necessary, of detected wrongdoing and vulnerability exploitation.

3.2 The following are examples of the types of files that the system owners shall review, as needed, for signs of wrongdoing and vulnerability exploitation:

3.2.1 Automated intrusion detection logs;

3.2.2 Firewall logs;

3.2.3 User account logs;

3.2.4 Network scanning logs;

3.2.5 System error logs;

3.2.6 Application logs; and,

3.2.7 Data backup and recovery logs.

3.3 Where feasible, a security baseline shall be developed for determining controls and access to information resources by conducting an annual security risk assessment, using tools such as the SPECTRIM System, by the ISO.

3.4 In accordance with UAP 29.01.03.P0.18 Information Resources – Incident Management, upon discovery of any security issues, a Security Incident Report Form will be completed and forwarded immediately to the ISO for follow-up investigation.

3.5 Any security issues discovered by any university faculty, staff, or students shall be reported in writing to the ISO for a follow-up investigation.

Related Statutes, Policies, Regulations and Rules

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

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

The Texas A&M University System Information Security Standards

Security Control Standards Catalog

Contact Office

Center for Information Technology Excellence 936-261-9350