

**PRAIRIE VIEW A&M UNIVERSITY
ADMINISTRATIVE PROCEDURES**

29.01.03.P0.12 Information Resources – Security Monitoring

Approved (May 26, 2009)

Next Scheduled Review (May-2012)

1. PURPOSE

- 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 the review of: user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

The purpose of security monitoring is to ensure that information resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

- 1.2 The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, 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 information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.
- 1.3 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.

2. DEFINITIONS

- 2.1 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.

- 2.2 Information Security Officer (ISO): responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).
- 2.3 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.
- 2.4 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, and failure to comply with regulations or legal obligations, or closure of the University or department.
- 2.5 Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Security monitoring of information resources shall be implemented based on risk management decisions by the resource information owner(s).
- 3.2 Mission critical or confidential information resource systems shall, at a minimum, enable operating system logging features. Automated tools shall be used where deemed beneficial by the resource owner based on risk management decisions.
- 3.3 Non-mission critical and non-confidential information resource systems may enable operating system logging features and other security monitoring features.
- 3.4 Network security monitoring will be conducted by Information Technology Services. Any other monitoring shall be coordinated with Information Technology Services, at 936-261-9300.
- 3.5 Logs and other data generated by security monitoring shall be reviewed periodically.
- 3.6 Where feasible, a security baseline shall be developed for determining controls and access to information resources by conducting an annual security risk assessment using the ISAACS tool.
- 3.7 Any significant security issues discovered and all signs of unauthorized activity shall be reported using the procedures detailed in the Incident Management procedure.

Contact Office: Information Security Officer; 936-261-2126