

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

29.01.03.P0.02 Information Resources – Backup Recovery

Approved (May 26, 2009)

Next scheduled review (May, 2012)

1. PURPOSE

- 1.1 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. 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 SAP 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.

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 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.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 The frequency and extent of backups shall be determined by the importance of the information, potential impact of data loss/corruption, and risk management decisions by the data owner (Department Heads and Information Security Administrators).
- 3.2 Mission critical information backup and recovery processes for each system, including those for offsite storage, shall be documented and reviewed periodically.
- 3.3 Physical access controls implemented at offsite backup storage locations.
- 3.4 Processes must be in place to verify that the actual offsite storage of mission critical data is taking place.
- 3.5 Backups shall be periodically tested to ensure that they are recoverable.

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