PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.02 Information Resources – Backup Recovery
Approved May 26, 2009
Revised August 29, 2013
Reviewed December 7, 2018
Next Scheduled Review: December 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to provide a set of procedures for implementing, monitoring, protecting, and testing of backup and recovery procedures for mission critical information and associated information resources that are stored in an electronic format. 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

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 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.

Official Procedures and Responsibilities

1. GENERAL

1.1 Electronic backups are a requirement to enable recovery of data and applications in case of events such as natural disasters, system disk drive failures, corruption, data entry errors, or system operations errors. However, such operational backups shall

not be used as a mechanism for meeting records retention requirements. The purpose of this UAP is to establish procedures for protection of electronically stored information.

1.2 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. 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) information resources that contain mission critical information. The intended audience for this UAP includes, but is not limited to, all PVAMU employees who are responsible for the support and operation of University information resources which contain mission critical information.

3. PROCEDURES

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 (i.e. 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. Additionally, all information resource owners should identify and ensure that all mission critical data is backed up by Information Technology Services (ITS) on a scheduled basis and stored off-site in a secure, environmentally safe, locked facility.

3.3 Physical access controls implemented at offsite backup storage locations shall meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest sensitivity level of information stored.

3.4 Information resource owners, in conjunction with ITS, must have a process in place to verify that the actual offsite storage of mission critical data is taking place.

3.5 Information resource owners, in conjunction with ITS, shall periodically test backups to ensure they are recoverable.

3.6 Backup media must have, at a minimum, the following identifying criteria that can be readily identified by labels and/or a bar-coding system:

3.6.1 System name;

3.6.2 Creation date;

3.6.3 Sensitivity classification of mission critical or confidential information based on applicable electronic record retention regulations; and,

3.6.4 Departmental information resource contact information.

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