

STANDARD ADMINISTRATIVE PROCEDURE

24.99.99.M1.06 Information Resources – Backup Recovery

Approved July 18, 2005

Revised February 24, 2009

Standard Administrative Procedure Statement

This SAP provides a set of practices for implementing, monitoring, protecting, and testing of backup/recovery procedures and associated information resources for mission critical information stored in an electronic format.

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.

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,
- determining controls and access to information resources supporting that business function.

Responsibilities and Procedures

1. GENERAL

Electronic backups are a requirement to enable the 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. The purpose of the University backup/recovery procedure is to establish the process for the backup and storage of electronic information.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to University resources that contain mission critical information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 24.99.99.M1.27 Exclusions from Required Risk Mitigation Measures.

The intended audience is all University staff 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.
- 3.2 Mission critical information backup and recovery processes for each system, including those for offsite storage, shall be documented and reviewed periodically. Additionally, mission critical data shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized TAMU representatives (TAC 202.74(b), 05/26/05).
- 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 Processes must be in place to verify the success of the information resource backups.
- 3.5 Backups shall be periodically tested to ensure that 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 based on applicable electronic record retention regulations; and,

3.6.4 departmental information resource contact information (reference [Record Management](#) for guidance/list).

Related Statutes, Policies, or Requirements

Supplements [University Rule 24.99.99.M1](#)

Contact Office

Contact [Information Technology Issues Management](#) for SAP interpretation or clarification.

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)
