Texas A&M University System Standard – Backup and Recovery

Standard Statement

This standard 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 System Office (SO) or information resource owner to be essential to the continued performance of the mission of the SO 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 department.

Information Resource Owner - An entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Responsibilities

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 SO backup/recovery standard is to establish the process for the backup and storage of electronic information.

2. APPLICABILITY

   This Standard applies to SO resources that contain mission critical information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard 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 standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience is all SO staff responsible for the support and operation of SO information resources which contain mission critical information.

3. STANDARDS

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 SO 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

Contact Office

Contact the Texas A&M University System Chief Information Officer or the Chief Application Architect for standard interpretation or clarification.

OFFICE OF RESPONSIBILITY**:** The Texas A&M University System Chief Information Officer