STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.06 Information Resources – Backup and Recovery

Approved July 18, 2005
Revised February 24, 2009
Revised November 5, 2012
Revised August 14, 2013
Next Scheduled Review: August 14, 2018

Standard Administrative Procedure Statement

This Standard Administrative Procedure (SAP) provides 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.

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.

Owner of an Information Resource - a person responsible for a business function and for determining controls and access to information resources supporting that business function.

Responsibilities and Procedures

1. GENERAL

   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 SAP is to

establish procedures for protection of electronically stored information.

2. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to university resources that contain mission critical information. The intended audience is all university employees who are responsible for the support and operation of university information resources which contain mission critical information.

3. PROCEDURES

3.1 Mission critical backup and recovery processes for each system, including those for off-site 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 facility accessible only to authorized Texas A&M University representatives as required by Texas Administrative Code, Title 1, Chapter 202, Information Security Standards.

3.2 The frequency and extent of backups shall be determined by the potential impact of data loss or corruption and, risk management decisions by the data owner.

3.3 Physical access controls implemented at off-site backup storage locations shall meet or exceed the physical access controls of the original source system(s). In addition, backed up information resources must be protected in accordance with the most restrictive classification of data that is being transmitted or stored. (For example if non-mission critical data files are combined with mission critical data files then the protection for all the backed up files must be at the mission critical level).

3.4 Where the original data source is required to be encrypted, the backup shall also be similarly encrypted.

3.5 Processes must be in place to verify the integrity of information resource backups. A backup and recovery test plan should be developed. The plan should ensure that the entire volume(s) or system of data stored from the originating information resource(s) is recoverable (i.e., ensure that an entire volume or system can be restored and not just one file). Backup and recovery procedures shall be tested at least annually to ensure that they are viable.

3.6 Backups in any form should be properly inventoried and be readily identifiable.

3.7 All electronically backed up information resources shall be sufficiently labeled and identified to enable staff to retrieve and protect data as needed.

4. EXCLUSIONS

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 *29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures*.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Chapter 202, Information Security Standards

Texas Electronic Records Standards and Procedures, State Agency Bulletin Number One, Section 6.93 Creation Electronic State Records.

System Regulation *61.99.01 Retention of State Records*

SAP *29.01.03.M0.01 Security of Electronic Information Resources*

SAP *29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures*

Texas A&M Information Security Control SC-13 *Cryptographic Protection*

Texas A&M Information Security Control CP-2 *Contingency Plan*

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY:

Associate Vice President for Information Technology & Chief Information Officer