29.01.03.H0.06 Backup Recovery

Approved: August 2011
Revised: January 2014
Next Scheduled Review: January 2019

Procedure Statement

Routine electronic backups of data and systems 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.

Reason for Procedure

Required by Texas Administrative Code, Chapter 202

This procedure applies to University information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this procedure is to provide a set of measures that will mitigate information security risks associated with the backup/recovery of information. 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 are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code, Chapter 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 procedure 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 (ISO).

The intended audience for this standard administrative procedure includes, but is not limited to, all information resources data/owners, users, management personnel, students and system administrators.

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): responsible for administering the information security functions within Texas A&M University-Texarkana and reports to the Information Resources Manager (IRM).

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.

Procedures and Responsibilities

1. Full backups will be performed weekly and differential backup daily on all critical data.

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.

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.

4. Processes must be in place to verify the success of the information resource backups.

5. Backups shall be periodically tested to ensure that they are recoverable.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

Contact Office

Department of Information Technology
903-223-3084