SAP 29.01.03.T0.04 Information Technology Services – Backup Recovery

Approved:	May 4, 2006
Revised:	February 28, 2012
Reviewed:	May 21, 2014
Next Scheduled Review:	May 21, 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 t this Standard Administrative Procedure (SAP) is to establish the process for the backup and storage of electronic information.

Reason for Procedure

This SAP applies to Tarleton State University information resources that contain mission critical information. The purpose of the implementation of this SAP 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 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 SAP 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 is all university staff responsible for the support and operation of university information resources that contain mission critical information.

Procedures and Responsibilities

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.

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.

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:
    a. system name;
    b. creation date;
    c. sensitivity classification of mission critical or confidential information based on applicable electronic record retention regulations; and
    d. departmental information resource contact information.

Related Statutes, Policies, or Requirements

Supplements SAP *29.01.03.T0.19 Security of Electronic Information Resources*
Supplements SAP *29.01.03.T0.01 Information Resources - Acceptable Use*

Definitions

1. **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.

2. **Information Security Officer (ISO):** responsible for administering the information security functions within Tarleton State University and reports to the information resources manager (IRM).

3. **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 division/unit. 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, noncompliance with regulations or legal obligations, or closure of the university or division/unit.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968-9395