TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.05 Backup and Recovery of Data

First Approved: March 28, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

Electronic backups are business requirements that enable the recovery of data and applications in case of events such as natural disasters, system disk drive failures, data entry errors, or system operations errors.

The purpose of this SAP is to establish the process for the backup and storage of electronic information. This SAP applies to all individuals within Texas A&M International University (TAMIU) who require a backup of a TAMIU-issued workstation, those who are responsible for the installation and support of Information Resources, individuals charged with Information Resources security, and data owners. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

---

1. Backup/Recovery

    1.1 The recovery process is outlined in the Disaster Recovery Plan.

    1.2 The frequency with which backups are created may vary depending on the importance of the information and the associated risks. Business owners are responsible for defining recovery time objective (RTO), recovery point objective (RPO), and frequency of backups.

    1.3 TAMIU's Information Resources backup and recovery process for each system must be documented and reviewed at least annually.

1.4 Backups will be verified through documentation that includes any logs generated by the backup application.

1.5 Backups must be periodically tested to ensure that they are recoverable. This process will be documented.

1.6 A full backup of the systems must be performed and stored offsite at least once a month.

1.7 Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the classification of the data (i.e., encryption of confidential or sensitive data).

1.8 TAMIU servers are backed up on a scheduled basis as outlined in the appropriate Standard Operating Procedure (SOP). Backups typically include both system-level and user-level data.

1.9 Users are responsible for creating backups of their own data. Such backups must be protected in accordance with the information classification of the data. OIT can assist data owners throughout the backup process. Owners, however, need to assess the following:

- value of the data,
- security and/or encryption requirements for the data,
- retention period for the backup, and
- specific needs or requirements for repetition of the backup.

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education
TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources
TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Definitions

Recovery Point Objective (RPO) - The interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold (source: Druva).

Recovery Time Objective (RTO) - The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity (source: Druva).

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310