Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.23	**Back-Up And Disaster Recovery Policy**	Responsibility:	Chief Information Security Officer

BACK-UP AND DISASTER RECOVERY POLICY

Overview

Creating a back-up of data that can be safely stored in another location is essential to business continuity in the event of loss of the computer system or media on which the data natively resides or unintended deletion or modification of the data. Each Information Resource Owner should ensure that data back-up processes and procedures are documented with defined recovery point and time objectives.

Policy

All UT Health San Antonio data, including data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner. A back-up plan must be documented and include procedures for:

1. Recovering data and applications in case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, system operations errors, or unauthorized access that modifies or deletes the data;

2. Assigning operational responsibility for backing up of all Servers;

3. Scheduling data back-ups based on recovery point and time objectives;

4. Establishing requirements for off-site storage;

5. Securing on-site/off-site storage and media in transit; and

6. Testing back-up and recovery procedures and integrity of back-up media.

Owners of Mission Critical Information Resources and of Information Resources containing Confidential Data must adopt a disaster recovery plan commensurate with the risk and value of the Information Resource and data. The disaster recovery plan must incorporate procedures for:

1. Recovering data and applications in the case of events that deny access to Information Resources for an extended period (e.g., natural disasters, security incident);

2. Assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions;

3. Testing the disaster recovery plan procedures every two years at minimum; and

4. Making the disaster recovery plan available to the Chief Information Security Officer and other stakeholders.

Accountability

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2, "*Handbook of Operating Procedures*".

Reference

- U.T. System Policy 165 Standard 8