I. POLICY STATEMENT

Electronic backups are a required business function necessary to enable the recovery of data and applications in the event of natural disasters, system disk drive failures, security incidents, espionage, data entry errors, or system operations errors and disruptions.

II. PURPOSE AND SCOPE

The purpose of the Backup/Disaster Recovery Policy ("DRP") is to establish rules for the backup and storage of electronic University information. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

The DRP applies to all individuals within the University enterprise who are responsible for the installation and support of Information Resources, and individuals charged with Information Resources security, and data owners.

The Office of Information Technology ("OIT") may maintain existing contracts for offsite backup data storage. These services may be extended to all University entities upon request.

III. DEFINITIONS

Not applicable.

IV. POLICY PROVISIONS

1. Backups must be performed at frequencies and scopes that align with the criticality of the information, the organization's risk tolerance, and the requirements established by the data owner.

2. The Information Resource backup and recovery process for each system must be documented and periodically reviewed.

3. Vendor(s) providing offsite backup storage for the University must be approved by the Information Security Officer to handle the highest level of information stored.

4. The alternate storage site must provide controls equivalent to those of the primary site.

5. A process must be implemented to verify the success of the electronic information backup. The frequency and extent of backups shall be commensurate with the classification and criticality of the information and the associated risk, as determined in accordance with institutional standards and Texas Administrative Code §202.

6. Backups must be periodically tested by OIT to ensure recoverability.

7. Procedures between the University and the offsite backup storage vendor(s) must be reviewed annually.

8. Backups must protect the confidentiality, integrity, and availability of stored information.

9. The University must maintain the capability to recover and reconstitute each information system to a known state following a disruption, compromise, or failure, consistent with institution-defined recovery time and recovery point objectives.

10. Disciplinary Action

Violation of this policy may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline & Termination Policy).

11. Applicable TSU Security Policy Standards

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22. Applicable security standards include, but are not limited to:

- Security Standard 1
- Security Standard 2
- Security Standard 3
- Security Standard 4
- Security Standard 5
- Security Standard 6