SECTION: Information Technology **Policy 04.06.07**
AREA: Information Security

SUBJECT: Backup/Disaster Recovery Policy

I. INTRODUCTION

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

II. PURPOSE

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 To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

III. SCOPE

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.

IV. SERVICES

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

V. POLICY

A. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

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

C. The vendor(s) providing offsite backup storage for the University must be cleared

by OIT to handle the highest level of information stored.

D. 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 highest sensitivity level of information stored as determined by industry standards and approved by OIT.

E. A process must be implemented to verify the success of the electronic information backup.

F. Backups must be periodically tested by OIT to ensure that they are recoverable.

G. Signature cards held by the offsite storage backup storage vendor(s) for access to backup media must be reviewed annually or when authorized individual leaves employment.

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

I. Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
   1. System name,
   2. Creation date,
   3. Sensitivity classification (based on applicable electronic record retention regulations), and
   4. University contact information.

VI. DISCIPLINARY ACTION

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

VII. 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 7
- Security Standard 9
- Security Standard 11

- Security Standard 14
- Security Standard 16
- Security Standard 17
- Security Standard 18
- Security Standard 19

VIII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer Billy Reeter

Review: Every year, on or before September 1

IX. APPROVAL

Jeri McShan

Vice President of Finance

President

2/18/11

Effective Date