Information Technology Security Plan
Backup Policy (10.13)

Responsible executive: CIO
Responsible office: ITS

Approval date: 7/01/2016
Effective date: 7/01/2016

Related policies: IT Security Plan, Server Security Policy

1.0 Policy Statement

All university data residing on systems maintained in the ITS data center must be copied onto storage media on a regular basis for the purpose of disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups.

2.0 Reason for Policy

The purpose of this policy is to provide guidelines for the continuity, restoration and recovery of data in the event of an equipment failure, intentional destruction of data or natural disaster.

3.0 Applicability

This policy applies to all university data residing on systems maintained in the ITS Data Center.

4.0 Terms and Definitions

Full Backup - creates a copy of every file on a storage device.

Partial Backup - creates a copy of selected files on a storage device.

Incremental Backup - creates a copy of files that have changed (i.e., modified or created) since the last backup was performed.

Differential Backup - creates a copy of files that have changed (i.e., modified or created) since a specific date and time.

Generation - a media rotation plan, where the media is kept for five backup cycles before the media is reused.

5.0 Policy
5.1 Data Backup Requirements

Information Technology Services (ITS) is responsible for the backup of data stored in the data center. The backup of data stored on individual workstations, whether they are university or personally-owned, is the responsibility of the user. Users should consult the Helpdesk for local backup procedures.

All mission critical data must receive a full backup on a daily basis.
System and application data are to be backed up with at least one full backup using the generation principle.

All weekly backup media must be stored in a fireproof safe.

All full backup media must be stored in an off-site backup archive storage location.

Each data backup process should have at least one primary backup administrator and one secondary.

Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.

The backup administrator should document the following items for each generated data backup:

- Name of backup media describing data contents
- Date of data backup
- Type of data backup (incremental, full)
- Backup administrator
- Storage location of backup copies

The restoration of data using data backups must be tested periodically to ensure that complete data restoration is possible to ensure whether:

- Data restoration is possible
- The data backup procedure is practicable
- Data backup procedures are documented properly
- The time required for data restoration meets the availability requirements