OLIVET NAZARENE UNIVERSITY | Information Technology

ENTERPRISE BACKUP POLICY

Approved Date: 1/27/2009

Policy Overview

This document defines the policy for the backup of computer systems housed within the Olivet IT data center and data on other servers for which Olivet IT is responsible

Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of disaster, equipment failure, or intentional destruction of data.

Scope

This policy applies to but is not limited to:

- File servers
- Print servers
- Mail servers
- WWW servers
- Application servers
- Internal management servers
- Directory services servers
- Document imaging servers
- Test environment servers
- University data and systems hosted by third-parties

Definitions

Backup: The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive: The saving of older copies of backup media for long-term storage.

Restore: The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

Full backup: A complete backup of all files on a system.
Incremental backup – Backup of only the files that have changed since the last full backup

Classification of Data

All data should be assessed and handled according to its importance to the operation of the University. Backup, rotation and testing will be performed to meet one of the following classifications:

a. Mission Critical – Data should be restorable to a state within the past 24 hours.
b. Important – Data should be restorable to a state within the past 72 hours.
c. Discretionary – Data should be restorable to a functional state.

Frequency of Backup

Backups are performed according to the mission criticality of the data.

Media Rotation

Media should be rotated amongst several sets with at least one functional set archived in an off-site location.

Restore Testing

Backups should be verified as readable after every backup job as part of the backup process. Periodic manual verification of readable data as needed.

Responsibility

The IT director will designate IT personnel to manage backup of University data.

Designated personnel is responsible for:

- Ensuring University data is protected according to this policy.
- Ensuring that University systems and data managed by third-parties conform to this policy or meet the standards of the third-party.
- Ensuring that data is corrrectly written to backup media.
- Verifying that data can successfully be recovered from backup media on a routine basis.

Data

Information backed up under this policy includes the following:

- Personal user data on network storage
- Server system data
- File permissions
- Directory data
- Specific software configuration

Archiving

Every 30 days a set of media should be kept off site in a secure location.

File Retrieval

File retrieval is primarily designed for restoring University operations in case of disaster or emergency. Reasonable user requests for file retrieval will be handled as if it were an emergency, provided the restoration of the file(s) falls within the above parameters and the process does not cause an inordinate amount of effort to restore.