Data Backup Policy

Purpose and Scope

- The purpose of this policy is as follows:
  - To safeguard the information assets of Wofford College
  - To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
  - To permit timely restoration of information and business processes, should such events occur.
  - To manage and secure backup and restoration processes and the media employed in the process.
- This policy applies to all servers in the Information Technology (IT) Data and Telephone Centers, including the Network Attached Storage (NAS)
- The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.
  - Backup retention periods are in contrast to retention periods defined by legal or business requirements.
  - System backups are not meant for the following purposes:
    - Archiving data for future reference.
    - Maintaining a versioned history of data.

Policy

- Systems will be backed up according to the schedule below:
  - Data stored on the NAS appliance will be regularly backed up as follows:
    - Incremental backup daily (Mon.-Fri.) and data located on-site.
    - Full backup weekly (Sat.) and data located off-site.
  - Exchange Mailbox stores will be regularly backed up as follows:
    - Full backup daily (Mon.-Fri.) and data located on-site.
    - Full backup weekly (Sat.) and data located off-site.
  - Banner will be regularly backed up as follows:
    - Full backup daily (Mon.-Fri.) and data located on-site.
    - Full backup weekly (Sat.) and data located off-site.
  - Windows Servers (not in DMZ) will be regularly backed up as follows:
    - Incremental backup daily (Mon.-Fri.) and data stored on-site.
    - Full backup weekly (Sat.) and data located off-site.
  - The Virtual Machine Server will have its VM data drive regularly backed up as follows:
    - Image backups of virtual machines will be taken on Tuesday and Thursday. These backup files will be stored on-site.
    - Weekly file and folder full backup will be taken on Sunday. These backup files will be stored off-site.

    - The Catalog tape will be regularly backed up as followed:
        - Full Hot Catalog backup daily (Mon.-Fri.) stored to Hard Disk on NAS.
        - Full backup weekly (Sat.) copied to tape stored off-site.
    - The Telephone system server will backed up as follows
        - Regularly on the first Monday of each month.
        - In certain circumstances when many changes have been made
            - The Panthers arrival and departure, for example.
        - Backup is made to a flash drive, as recommended by Ericcson, which is stored in the safe in Roger Milliken Science Center
- Backup tapes will be transported and stored as described below:
    - Currently all backups will be written to reusable LT03 media with capacity of 400 GB uncompressed (800 GB compressed) and a transfer rate of 60 MB/Sec (native).
    - Media will be clearly labeled and stored in a secure area that is accessible only to IT staff or employees of the contracted secure off-site media vaulting vendor used by IT.
    - During transport or changes of media, media will not be left unattended.
    - Daily backups will be stored on-site in a physically secured fire-proof safe located in a building separate from the Data Center.
        - Daily backups will be maintained for one week.
    - Weekly backups will be stored in a physically secured, off-site media vaulting location maintained by a third party.
        - Weekly backups will be maintained for a period of three weeks.
        - After the period of three weeks has elapsed, the tapes will be returned to IT and will be either re-used or destroyed.
- Media will be retired and disposed of as described below:
    - Prior to retirement and disposal, IT will ensure that:
        - The media no longer contains active backup images
        - The media's current or former contents can not be read or recovered by an unauthorized party.
    - With all backup media, IT will ensure the physical destruction of media prior to disposal.
- Backups will be verified periodically.
    - On a daily basis, logged information generated from each backup job will be reviewed for the following purposes**:**
        - To check for and correct errors.
        - To monitor the duration of the backup job.
        - To optimize backup performance where possible.
    - IT will identify problems and take corrective action to reduce any risks associated with failed backups.
    - Random test restores will be done once a week in order to verify that backups have been successful
    - IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

- Data Recovery
    - In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.
    - In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.
- Restoration Requests
    - In the event of accidental deletion or corruption of information, requests for restoration of information will be made to Ron Wood.

Responsibilities

• Backups and Date Recovery	Matt Fisher, 597-4274
• Telephone System Backups	Chris Myers, 597-4279
• Verification	Matt Fisher, 597-4294
	Ron Wood, 597-4273
	Bryan Blackwell, 597-4272
	Reba Epton, 597-4270