**Data Backup Policy**

# Purpose and Scope

* The purpose of this policy is as follows:
  + To safeguard the information assets of Norserage
  + 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.
* 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:
  + Linux Machines 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 on-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 on-site.
* 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, on-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 IT Team.

This policy was modeled after: http://dept.wofford.edu/it/Data%20Backup%20Policy.pdf