University of Wisconsin La Crosse Backup and Restoration Guideline

Executive Summary

System Backups:

- Each server is completely backed up at least once each week
- Each server is incrementally backed up every night
- Data backups stored on easily accessible media in Wing Technology Center and also copied to a secondary location on campus
- Regular daily backups are kept for 30 days, end of month backups are kept for 6 months
- Data older than 6 months is not retrievable

Restore requests should be directed to the Eagle Helpdesk (608) 785-8774. Due to the nature of periodic backups, if a file is created and destroyed between backup windows, the file may not be recoverable. Typical recovery times can take between two and four days. Restored data will be made available to users as soon as possible, but the timeline previously noted is approximate and is not guaranteed.

Purpose and Scope

- The purpose of this guideline is as follows:
  - To safeguard the information assets of University of Wisconsin La Crosse
  - 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 guideline applies to all data stored on servers and on the SAN in Information Technology Services (ITS)
- 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.
  - This guideline meets or exceeds the backup provisions of the UW System - General Records Schedule for IT records. Other requirements addressed by the

General Records Schedule for IT records must be adhered to as well, but are not in scope for this guideline.

Guideline

- Systems will be backed up according to the schedule below:
  - Servers will be regularly backed up as follows:
    - Incremental backups are performed daily, with exception to the one day a full backup is performed
    - Full backups on all systems are performed one day each week
      - All servers follow the above backup schedule unless noted otherwise according to the server owner and documented on BackUp_Server_Info.xlsx
    - All data will backup to disk in the Wing Data Center and will be replicated to a second set of disks in the Murphy Data Center daily.
      - Data will be retained on disk for approximately 30 days
    - The last full backup performed at the end of every month is considered a Monthly backup.
      - Monthly backups are written to one set of removable media, kept for six months, and are stored off campus but easily accessible.
      - Monthly backups are also written to a second set of removable media, this media is for catastrophic failure
        - kept for one month and are stored off campus at least 75 miles from campus

Media

- Removable media will be transported and stored as described below:

  - Currently all monthly backups will be written to two sets of reusable removable media
  - Monthly backups will be stored in a physically secured room in a building separate from the Wing Data Center and separate from the Murphy Data Center until taken to two separate off-site locations.
    - Monthly backups will be maintained for a period of six months.
      - After the period of six months has elapsed, the removable media will be returned to ITS and will be either re-used or destroyed.
    - Monthly tapes used for catastrophic failure will be maintained for a period of one month.
      - After the period of one month has elapsed, the removable media will be returned to ITS and will be either re-used or destroyed.
  - During transport or changes of media, media will not be left unattended.

- Media will be retired and disposed of as described below:
  - The date each removable media was put into service shall be recorded on the removable media, so as to know the age of the removable media (starting December 1st, 2010)
  - Prior to retirement and disposal, IT will ensure that:
    - The media no longer contains active backup images
    - The media's current or former contents cannot be read or recovered by an unauthorized party.

- With all backup media, ITS will degauss the media. After media is degaussed, it will be sent to a e-waste recycling company for the physical destruction of media, at which point it will be shredded.

- **Restoration and Time Expectations**
  - Due to the nature of periodic backups, if a file is created and destroyed between backup windows, the file may not be recoverable.
  - Typical recovery timelines are as follows:
    - Restore point in time of 30 days or less can be expected to take up to two business days
    - Restore point in time greater than 30 days can be expected to take up to four business days
    - Restored data will be made available to users as soon as possible, but the timelines noted above are approximate and are not guaranteed.
  - In the event of a catastrophic system, non-catastrophic system failure or user error all attempts will be made to restore data, but is not guaranteed.
  - **Restoration Requests**
    - In the event of accidental deletion or corruption of data, requests for restoration of data must be made to the help desk.
      - Requests should include information about the file- approximate creation time if created within the last 24 hours, name of the file, location of the file, last time it was changed, and date and time it was deleted or destroyed.

- **Guideline and Backup testing**
  - Backups will be verified periodically.
    - On a daily basis, logged information generated from each backup job will be reviewed for the following purposes**:**
      - To verify success or failure of backups.
      - To check for and correct errors
      - To monitor the duration of the backup job.
      - To optimize backup performance where possible.
    - ITS will identify problems and take corrective action to reduce any risks associated with failed backups.
- Test restores will be done at least once a month in order to verify that backups have been successful and will be documented in Backup Verification.xlsx

- **Definitions**
  - Full Backup- Backup of all files and folders
  - Incremental Backup- An incremental backup contains only data that is new or has changed since the last backup, regardless of the type
  - Monthly Backup- the last full backup performed at the end of every month
  - Restoration- a process that involves copying backup files from secondary storage (tape or other backup media) to hard disk. A restore is performed in order to return data to its original condition if files have become damaged or to copy or move data to a new location.
  - Corruption- refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data

- Removable media- refers to storage media which are designed to be removed from the computer without powering the computer off.
- Degauss- Data is stored in the magnetic media, such as hard drives and magnetic tape, by making very small areas called magnetic domains change their magnetic alignment to be in the direction of an applied magnetic field. Degaussing, commonly called erasure, leaves the domains in random patterns with no preference to orientation, thereby rendering previous data unrecoverable
- Catastrophic- is an extremely large-scale disaster

- **Revision History**
  - DRAFT
  - DRAFT v.2 9/15/2011
  - DRAFT v.3 11/15/2012
  - DRAFT v.4 11/26/2012
  - DRAFT v.5 11/27/2012
  - DRAFT v.6 9/29/2014
  - DRAFT v.7 3/7/2016