Data Backup Policy

Purpose:

- To backup all data stored on Franklin W. Olin College of Engineering servers.
- To prevent the loss of and permit timely restoration of critical data in the event of an accidental deletion, corruption of data, system failure, or disaster.
- To manage and secure backup and restoration processes and the media employed in the process.

Scope:

- This policy applies to all Olin College servers/systems managed by the Information Technology Department (IT).
- This policy does not apply to individual end user systems, personal systems or systems not owned/managed by the College.
- 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.
- Backups are not meant for the following purposes:
    - Archiving data for future reference;
    - Maintaining a versioned history of data.

Policy:

- Retention:
    - Standard system backups are retained for four weeks for recovery purposes only.
    - Long term backups for monthly and/or other business requirements are copied to magnetic tape or CD/DVD media:
        - Business units are responsible for identifying and communicating all non standard backup needs and working with the IT Dept to achieve them.
        - Monthly backups are retained for one calendar year
        - Backups for regulatory requirements are retained for the period defined by such requirements
- Tape and CD/DVD media is transported to and stored in a safe located in a secure room in another building.
- Tape and CD/DVD media is reused and overwritten as necessary.
- All media to be disposed of shall be sufficiently and securely erased and destroyed so as not to be able to retrieve any data prior to disposal.
- All IT managed servers are backed up nightly to a disk based appliance with RAID 5 and data deduplication.
    - A full system backup is performed once weekly;
    - Differential backups are performed daily between weekly full backups;
    - Exchange environment: A complete backup of the Exchange information store is performed daily.
- Virtual Machines (VM's):
    - Snapshots: (Can't be used as a standalone backup for recovery):
        - Shall be made as necessary as determined by system administrators, application managers and/or IT management and typically for short term rollback/recovery needs;
        - Shall be maintained only as long as necessary and then removed.
- System Administrators shall check backup event logs and reports on a daily basis to ensure proper backups and take appropriate action to correct any problems.
- System Administrators shall perform file/system recovery tests using random files from backup monthly.
- End users:
    - Are strongly encouraged to store institutional data on centralized systems that are regularly backed up;
    - Are responsible for maintaining copies of data stored on their own system(s);
    - End users shall call or submit an email request for all data recovery needs to the IT Help Desk.