

I. Purpose and Scope

- The purpose of this policy is as follows:
 - To provide secure storage for data assets critical to the work flow of official university business
 - To prevent loss of data in the case of accidental deletion / corruption of data, system failure, or disaster
 - To permit timely restoration of archived data in the event of a disaster or system failure
- This policy applies to all computers, both mobile and desktop, owned by the Library
 - Specific locations will be automatically backed up (e.g., My Documents, Desktop, Bookmarks)
 - Any location outside of the automated backup locations will be added on a per request basis
- Backups are NOT meant for the following purposes:
 - Maintaining a versioned history of data
 - Personal data such as photos, videos, music, non-brown e-mail accounts, etc.
 - Programs (i.e., applications) of any type (personal or officially supported)
 - Exceptionally large images (scanned or digitized material) and large video files. If you need this type of storage space, please contact Libtech to discuss alternative backup options available to you

II. Backup and Recovery Policy

Data

The following resources are made available to backup critical files pertaining to official university business:

- \\filese.ad.brown.edu\library_users - scroll down to your user folder (e.g., jcarberry)
Secure storage for staff documents, presentations, spreadsheets, etc. pertaining to official university business.
- \\filese.ad.brown.edu\library_shared - scroll to dept. folder (e.g., _Systems_Office)
Secure storage for departmental and shared usage
- External USB hard drive
Utilizing Microsoft Backup or Apple's Time Machine to backup user folders that are in excess of the TWO Gigabytes . A member from Libtech will perform the initial configuration and schedule a backup policy. All external drives must be locked in a secure location at the end of the work day.

- **USB Thumb drive**
Not supported as an official means of backup. These devices can easily be misplaced or lost resulting in the potential breach of official university data. If utilized, the data must be encrypted if taken off the premises.

Archived E-mail

The university has recently moved to GoogleApps for e-mail and has provided a dynamically growing 7+ Gigabytes of e-mail storage (including attachments). If your archived e-mail is larger than the allotted storage space, it will be treated on a case-by-case basis. CIS is also actively searching for a service that supports online e-mail archival for more than 7 Gigabytes.

Archived e-mail stored on your computer's hard drive is not backed up if it does not fit one of the templates in the data backup policy above. Please contact someone from Libtech to assist with a backup option.

Backup Schedule and Retention

The Legato NetWorker backup system is utilized to retain data for 6 weeks or 42 days. A combination of incremental and full backups is executed on the dataset. A full backup is performed every Friday with incremental backups thereafter.

This creates a scenario where CIS can restore a folder like \\filese.ad.brown.edu\library_shared\systems_office to a single point in time in the past up to a maximum of 42 days.

Software

Windows Operating System:

Microsoft Backup is utilized to backup to, restore from, and verify data on the PC platform

TrueCrypt – open source on-the-fly data encryption for drives (provide more detail...)

AxCrypt – open source file level encryption

Macintosh Operating System:

Time Machine is utilized to backup to, restore from, and verify data on the Macintosh platform

TrueCrypt – open source on-the-fly data encryption for drives (provide more detail...)

FileVault – is utilized to encrypt at the file level using AES-128 bit encryption

Verification

If configured properly, both Time Machine and Microsoft Backup will perform a full verification against a backup set after every job to protect against corrupted data. No other form of verification is scheduled or performed.

Data Restoration

Emergency recovery: Systems staff will make every attempt to recover the data within a business day. However, in the event of a catastrophic event, such as fire damage, services and data may be unavailable for an extended period of time.

Non-Emergency recovery: These restorations will be performed on a time available basis, and will occur within the next five business days.

Required Information: Users that need files restored must submit a help desk ticket request or contact Libtech@brown.edu. The detail of the request should include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

- ❖ **Any lost data not backed up is beyond the scope of this document**
- ❖ **You are responsible for saving files to the specified backup directories**