CUNY Graduate Center
Information Technology

IT Backup and Restore Policies
Last Updated: September 16, 2020

Purpose and Scope

The purpose of this document is to describe the current data backup policy at the Graduate Center and the ASRC locations in the event of system failure, accidental deletion, corruption, or disaster. If such events occur, timely restoration of information and business processes is required.

This policy applies to user data on production servers at GC\5th administered by Information Technology. This policy does not apply to user data on non-IT servers, desktop computers, or test/dev servers hosted by IT.

The retention periods of information contained within a system-level backup are designed for recoverability and provide a point-in-time snapshot of information as it existed during the period defined by system backup policy.

Email Exchange (Faculty/Staff)	28 days
Application Servers/Databases	28 days
Windows File Shares/Other Data	28 days
Linux User files	30 days

Data Backup

- Data stored in production MS/SQL Server databases (SharePoint, EventPro, Track-It! etc.) is backed up at GC\5th continuously and recoverable for 28 days at the GC. These backups are copied offsite to GC\ASRC nightly and kept for seven days. Also, S: drive folders and private folders on the file server and MS/SQL Server data are replicated throughout the day from GC\5th to GC\ASRC. Microsoft SQL server is backed up twice a day.
- Windows Servers with frequently changing data are backed up daily at GC\5th, and these backups are retained for 28 days; these backups are copied offsite to GC\ASRC nightly and kept for seven days. This includes: Departmental shares (S: drive and private folders), Email, etc.
- Windows Servers with "static" data are backed up weekly and retained for four weeks at the GC; weekly backups are copied offsite to GC\ASRC and kept for two weeks. Retention of offsite backup copies is constrained by limited backup capacity at GC\ASRC.
- Transaction logs of production MS/SQL servers are backed up every 180 minutes and kept for 28 days.
- Windows Servers (in DMZ): Daily if the data changes frequently or weekly if the data changes infrequently.

- Linux servers with frequently changing data are backed up twice every night using different techniques at GC\5th, and these backups are retained for 28 days; these backups are copied offsite to GC\ASRC nightly and kept for seven days
- Linux servers with static data are backed up weekly using two different techniques at GC\5th, and these backups are retained for 4 weeks; these backups are copied offsite to GC\ASRC and kept for 2 weeks.
- User files on Linux Servers are backed up daily and kept at the GC/5th for 30 days.
- The telephone system configuration is backed up daily.
- Backups of surveillance videos are not required.

Data Recovery:

- Users may self-restore recent files (including prior versions) on department shares (Groupwork — S: drive) for up to one month and recover email in the deleted folder up to 1 week after deletion. IT can restore files, emails, and other data from backups within 28 days of deletion upon request. Users can self-restore from SharePoint for **30 days**, and IT can restore SharePoint for **60 days** upon request.
- Backup of videos from Security video cameras are made and retained on a "best efforts" basis and are not copied to GC\ASRC.
- IT does not backup data on PC or MAC desktops or GC-owned laptop with a GC property tag. IT does not backup data in computers located in research labs. IT does not backup any cloud-hosted data.