Academic Technologies Procedures and Recommendations 2019

I. Preservation of Data

Most departmental directories and individual home directories are on the Office of Information Technology (OIT) storage infrastructure. This network storage is backed up by OIT.

- Your deleted files are easily restored via nightly "snapshots" within 14 days.
- Snapshots run at night, so files created during the day and deleted on the same day are not available for restoring
- Up to 7 versions of files (and one copy of deleted files) are backed up to another data center for 6 months before they are permanently eliminated.
- A backup of current file versions is, of course, always kept.
- Note that, due to the amount of data on the law school's network storage, backups run continuously. They do not currently capture new files every day. Depending on when your file was created, it may need to be on the server for two weeks to be backed up.

Our snapshot and backup service is provided only for files stored on the network servers. This includes drives G: and J: on faculty and staff computers, and the R: drive on the student journal computers. Faculty and staff members who require backup for files on their hard drives (e.g., drive C:) should contact the Academic Technologies helpdesk for recommendations.

The Academic Technologies department also provides archive and media storage, which is replicated to a second data center.

The Clinics server is backed up and encrypted separately to ensure data isolation.

II. Network Resources

1. All law school members are given accounts on Duke's Office of Information Technology's Exchange email service.

    - All law school faculty and staff members are assigned full name aliases in the law.duke.edu domain (e.g., FirstName.LastName@law.duke.edu). All faculty members are also assigned last name aliases (LastName@law.duke.edu), which are by default their preferred addresses (i.e., what Exchange uses as their From: address).
    - Student members of the community are assigned full name aliases in the lawnet.duke.edu domain (e.g., Firstname.LastName@lawnet.duke.edu). Lawnet aliases and email forwarding are also available to alumni. Students can retain their lawnet addresses throughout their student career and as

alumni.

2. Email systems are bounded by limits in processing and storage space. If you outgrow your quota on Outlook, you may wish to archive messages. Our recommendation:

    - Configure Outlook for Windows to create an email archive *manually* on your home directory (e.g., J:); by doing so, you can be sure that the archive is backed up and can make it accessible to multiple computers. To access your archives from computers other than your office desktop Windows computer, first copy the archive to a local drive on that computer and then open it (Windows) or import it (Macintosh).

3. Networked file storage is designed to provide a secure and convenient location for storage of important data files. Because file servers are securely backed up, they are expensive and limited resources. The following guidelines are designed to help us allocate them efficiently.

    - Keep personal file storage below 5GB, excluding any Outlook archives.
    - Only store your own *data* files (no applications, installers or other sorts of "backups" that are not your own data).
    - Only store data files relevant to your role at the law school. We know that media files can be relevant to instruction and other work, but please find alternate storage for personal music, photo and video libraries. We can provide advice on ways to back up and keep these libraries safe.

    If you anticipate that your storage needs will grow substantially, please contact the Academic Technologies helpdesk so that we can work with you and assure the best solution for the need.

III. Network Security

The law school network uses Microsoft Windows and Linux operating systems on servers. Data transmitted over the network is protected by encryption, and data stored on the network is controlled by the use of user account restrictions. Nevertheless, personal and institutional data are potentially at risk from unauthorized users. If an unauthorized user obtains access to your files, any of the following could happen:

1. **Data Corruption.** Your files and those in any shared directories to which you have access could be altered or destroyed.
2. **Unauthorized communications.** Through local email and the law school's connection to the Internet, email could be sent under your name, files could be transferred to or from your directory, and charges could be incurred for uses of fee-based electronic services.
3. **Release of information.** Unauthorized persons could access and release your confidential or private data, or the confidential and private data of others.

Network security depends on the actions and concern of each individual user of the network. Because both personal and law school data can be placed at risk if network security is not taken seriously, the law school has adopted the following policies and recommended practices.

IV. Computer Security

There are two basic categories of law school-owned computers: *Office desktop computers* are fully managed, meaning that their core software is installed and updated by Academic Technologies. *Laptops and home desktops* are now also fully managed. However, how security updates are installed will differ between these two groups.

Another difference lies in levels of access. In general, all faculty and staff members are expected to access their computers with user-level accounts, since this level of access will limit the possibilities for breaches of security. We do issue local administrative accounts to all laptop/home desktop users so that they do maintenance when they and their computers are away from the law school. By request faculty members can also get a local administrator account on office desktop computers.

To prevent unauthorized access to your files, you should lock your computer through logging out or a screen saver that requires login whenever leaving it for more than a brief period. Your office should be locked when you are away to protect against both unauthorized use of the computer and physical theft. All drives should be full desk encrypted. Multi-factor authentication should be activated in all ways possible for staff who work with confidential information. Those who work in publicly accessible areas should use quickly activating screen savers with password protection; we also recommend screen filters to prevent others from seeing screen contents.