

## Computer Systems Security & Backup

The Hauppauge Public Library requires that their computer systems maintained by Network Administrator fall under one of several backup profiles as described below. The purpose of a systems backup is a level of business continuity of our computer system in the event of a hardware/software failure, physical disaster, or human error.

The Hauppauge Public Library uses a backup solution called Datto. A Datto backup consists of a full image and perpetual incremental snapshots. A full backup contains a bootable image file that consists of every file on the system. In the event of a system failure, the image is bootable and can immediately take the place of the failed system. An incremental backup includes only those files that have changed since the last full backup. Each increment is appended to the full image, making all incremental snaps bootable as well.

Backups are performed on a periodic schedule as determined by the library or application owners in conjunction with Network Administrator. The current Datto backup schedule is as follows; one snapshot every hour between the hours of 8am and 9pm seven days per week. This allows us to restore to the previous hour and file or complete system loss.

Backups are kept in two separate locations. One copy is kept onsite on the Datto device for quick data recovery. The other copy is replicated offsite, and outside the local geographic area for protection in the event of a regional disaster. In the event of a major disaster, offsite images are also bootable. Offsite data is transmitted and stored in an encrypted format. Onsite backups are kept for three months; offsite backups are retained for 1 year.

**IMPORTANT:** Backups save a copy of data, files, and directories found on the disk at the point in time the backup was performed, but do not record all activities or contents of users' files throughout the day. As a result, it is completely possible for a user to create and delete a file during the course of a day which will never appear on a backup. It is also important to note that a system backup is not intended to serve as an archival copy or to meet records retention requirements. Those needs are dictated by library policies and typically require dedicated hardware/ software solutions or other outlined processes.

### I. System Backup Profiles

- 1) Accounting Backup: The accounting backup provided for the system running financial software is as follows:
  - a) A full backup is initially performed on the accounting user's documents and files.
  - b) An incremental backup is performed every four (4) hours and saved on and off-site.
- 2) Network System Backup: Certain library-wide systems are necessary for public or staff stations to function. Systems that fall into this category include the servers. The backup schedule for these systems is as follows:
  - a) The server is backed up hourly between 8am and 9pm, seven days a week.
  - b) Backups are to be saved onsite and sent offsite upon completion.
- 3) No Backup: If a system does not fall under any of the backup profiles listed above, it may not be backed up.

## **II. Virus Protection**

All staff computers must have an anti-virus installed with the latest available virus definitions. Public computers must have their firewalls enabled, and be set to clear all changes upon the end of a user session (via DeepFreeze).

## **III. Firewalls**

Public computers must have their firewalls enabled to prevent the potential spread of computer viruses. The only firewall exclusions enabled by default will be for DeepFreeze administration and PC Reservation (Guest management software) server communication.

## **IV. Account Permissions**

Only accounts requiring domain administrator access will be granted access. This includes Network Administrator and the Chief Executive Officer.

Staff who have a dedicated computer may be made a local administrator of such computer upon request if a need is demonstrated.

Each staff user will have access to a shared network location. The shared location will be public among staff. Staff with a private login will also have access to a private home directory. The home directory is a second network location that is private with respect to staff but accessible by the Chief Executive Officer.

## **V. Administrative Rights and Passwords**

Network Administrator and Chief Executive Officer will both have copies of all passwords for network hardware and software, servers, Guest and print management systems, back-up systems, filters, and any other related security or system controls.

Adopted: March 25, 2014

Amended: April 20, 2017; June 2021