Computer Systems Security & Backup

The Sayville Library requires that their computer systems be maintained by Network Administrator falling under one of several backup profiles as described below. The purpose of a systems backup is to provide a means to restore the data of a computer system in the event of a hardware/software failure, physical disaster, or human error.

A system backup consists of either a full backup or incremental backup. A full backup contains every file on the system, whereas an incremental backup includes only those files that have changed since the last full backup. Backups are preformed on a periodic schedule as determined by the library or application owners in conjunction with Network Administrator.

Onsite backups are typically stored on a dedicated storage device. Once the backup retention period expires, the data is overwritten, erased, or destroyed in an approved manner.

Backups of the servers are kept in two separate locations. One copy is kept onsite in the Technical Services network room for quick data recovery. The other copy stored offsite with an online backup service, and outside the local geographic area for protection in the event of a regional disaster. Data is stored and transmitted in an encrypted format. Onsite backups are kept for one month, offsite backups are retained indefinitely.

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.

System Backup Profiles

1. **Accounting Backup:** The accounting backup provided for the systems (sayb and slsql servers) running financial software is as follows:

- A full backup is initially performed on the accounting user's documents and files weekly
- An incremental backup is performed during the work day 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 sayfs server. The backup schedule for these systems is as follows:

- The network shares of saylib (user data) to be backed up nightly.

- Backups are to be saved onsite and sent offsite upon completion.

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).

Firewalls

Public and staff 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 iTeam (patron management software) server communication.

Account Permissions

Only accounts requiring domain administrator access will be granted access. This includes Network Administrator and the Library Director.

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 Library Director.

Administrative Rights and Passwords

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

Adopted: 10/14/14