TECHNOLOGY COMMITTEE PROCEDURES

Committee Responsibilities

The committee is responsible for overseeing computer and network operations.

The committee reports to the board about new technology ideas and any major changes to the IT framework.

The library director approves all purchases. A committee member acknowledges receipt of all new hardware/software. These purchases are then approved by the board on the warrant list.

Back-Up Plan

QuickBooks

- Backups will be made whenever the bookkeeper makes changes
- The bookkeeper will take one copy offsite. In addition, the software allows for a copy to the QuickBooks online backup service. Another backup will be placed on a flash drive and kept in a locked cabinet.

Library Circulation System

- These files include all cataloging and circulation activities for the library's collection.
- These files are maintained offsite by the library system.
- The library system has responsibility for backing them up as part of the library's agreement with them.

All Other Files

- These include correspondence, board records, historical records, and daily business.
- These are maintained in a cloud account.
- In addition, a hard drive backup is made once a week and maintained offsite.
- A mailing database with patron addresses will be kept on a thumb drive in the locked cabinet unless in use by staff.
- A Friends of the Library database of members will be password protected
- Civil Service documents with staff information will be placed on a thumb drive and moved into the locked cabinet.

User Accounts

The director, bookkeeper, cataloger, and Friends Group shall have access to special user accounts on the primary staff computers that they use. Otherwise, staff will share a user account on the circulation desks. The Mid-Hudson Library System IT Staff maintain administration user accounts on all computers as they provide IT support.

Each staff member will have an individual login in the online circulation system. However, the Library recognizes because of the difficulty of logging off/on that staff members may be sharing a login on a given day. When an employee leaves the Library, the system will be notified that their login is no longer valid. User accounts that have not been used within a year will be deleted from Sierra. Staff change their ILS logins every six months.

Data Security

Segregate staff areas of the network from patron access from public computers and the WiFi. Staff are only given access to user functions in Sierra that they need to perform their jobs. Staff are also limited by their job title to the files that they have access to on the network.

See Back-Up plan for sensitive data for Quickbooks and the Library Circulation System.

Financial transactions made using a public web server must use Secure Sockets Layer (SSL).

Computers are sent to the Library System to be wiped of data before being disposed of. Flash drives are erased before being shared.

A password encryption program will be used to store and develop copies of the Library's passwords. The Mid-Hudson technical support staff shall have emergency access to this program and its contents.

Sierra passwords will contain complexity requirements. They should be at least eight characters and contain an uppercase character, a lowercase character, a numeric character, and a special character. These passwords are changed every six months.

Discourage users from writing down passwords. Default passwords for servers and applications are changed.

Software Security

- Test software before general dissemination to patron computers.
- Only install software necessary for local government business.
- Restrict rights to download or install software to as few individuals as practical.
- IT administration should backup software by securing the master copies of the software and its user instructions.
- Give licensed software only to appropriate users who need it to perform their duties.
- Maintain an inventory of software applications installed on all computers.

Network Security

- Utilize virus protection and ensure all computers have an up-to-date version.
- Ensure updates to servers, the operating system, and applications are done in a timely manner.
- We allow access to our WiFi system, but secure our staff network from access from the WiFi.
- Remote access is not available.
- Steps shall be taken to secure equipment, which is taken offsite. This includes not leaving equipment in unlocked cars or in public places.
- The network room is locked and only the staff/board have keys. There are no windows or outside doors in this room. The room is air-conditioned.
- Plug all equipment into surge protectors and use an uninterrupted power supply (UPS) or a backup power source.
- Maintain and repair equipment as needed.
- For small networks, router & firewall are functionally synonymous. We have an effective firewall in place.
- Review activity logs recorded by the firewall and IDS: Firewall logs are available on your router and reviewed when MHLS does service visits or makes changes. Given the lack of particularly critical resources on the network, it can honestly be argued that's sufficient proportional to the needs of the network.
- All ports are closed except those needed.
- Ensure that vendor access to the network is restricted only to files and applications needed to perform their duties: III has no access to your files. Comprise only has access to the command PC.
- Safeguard highly portable equipment in limited access cabinets or storerooms when not in use.
- Steps shall be taken to secure equipment, which is taken offsite. This includes not leaving equipment in unlocked cars or in public places.
- Unless noted otherwise, the director is responsible for physically safeguarding equipment.

Patron Security

Circulation System:

The system used by the West Hurley Public Library to circulate materials is a cloud-based system. The terminals in the library only access this data. As a result, security is maintained by the Mid-Hudson Library System, III, and AWS.

> From the Mid-Hudson Library System (11.1.19): The ILS (Sierra) is hosted with III and AWS, who work to maintain a high level of security. MHLS, III, and AWS all carry cyber insurance that covers the ILS. No patron information is stored locally on the client PCs. As such, member libraries do not need to obtain their own coverage.

Records about patron borrowing activity are kept as minimal as possible. Patron records include the items currently borrowed as well as items with current and past fines and fees. Item records include information about the current borrower and the previous borrower. Patrons may opt in to a "reading record" of their material from their online login. Member library staff cannot opt in for them or view this historical reading data.

Computer Usage:

A product called SAM by Comprise is used for patron computer reservations and computer printing. Information about patrons is download to a server in the computer closet.

> From Daniel Curtin, President of Comprise (10.24.19): As I understand it, our Cyber Liability Policy covers our products wherever they reside. Additionally, I would suggest that a customer using only SAM has little or no CL exposure because SAM does not record any combination of Personally identifying Information, it does record Patron Name, but name alone is not typically considered a threat.

SAM imports Patron Name, DOB, and library card number from the ILS. In order to further protect the security of our patrons, the technology committee decided to enable SAM Privacy Manager. While this will not eliminate the presence of patron records on your SAM server, it will sever the connection between a patron record and the statistical data this is collected (how much time a particular patron used and what computer on what day was used by a particular patron).

A product called CIPA filter is used to filter Internet websites. The system currently maintains one seven-day backup of web reporting data (every Saturday) plus whatever is currently in the file. Previous backups are deleted when the new one is made. There aren't any usernames on the devices, so the information consists of a list of sites visited. This report is only available to someone with administrator access. Otherwise, it is extremely difficult to get into the filter. (Information current as of 10.30.19)

Databases:

The Library has subscriptions and links to reputable third-party external services with their own privacy policies and requirements for creating accounts. These companies offer services including eBooks, streaming content, online learning, and online articles and magazines. You are encouraged to review the privacy policies for these services.

eNewsletter:

The library uses the company MailChimp to send out eNewsletters. Patrons must agree to be added to this service before they are added to the service. Patrons can opt out at any time. Mailchimp, in turn, takes steps to protect the patron data that is stored in their servers.

Website:

Statistical summaries are reviewed to learn how electronic services and web pages are used in order to improve website content, improve services, and troubleshoot problems.

Examples of statistics gathered:

- Referring site or site last visited
- Time and date of user sessions or visits
- Browser types and versions in use
- Operating systems in use
- Internet Protocol (IP) addresses assigned to Internet service providers

Items too Diffficult (or Costly) to Implement

- Mark or label all equipment as property of the local government. (We mark items without serial numbers.)
- The overall security plan should include a disaster recovery plan. This plan could include an alternate processing location and a plan to procure computers with the appropriate software to resume normal operations.
- Notifications for adding/removing users should be retained (Organization too small to track paperwork)
- Passwords should contain complexity requirements. (Sierra passwords will. When possible, a password security program will be used.)
- Disguise passwords upon entry into the computer. (Software dependent)
- Require users to log off their account before stepping away from the computer and require users to shut off computers before they leave for the day. (Sierra needs to remain up for staff to use.)
- Lock user accounts after three to seven consecutive attempts with an incorrect password. (Software dependent)
- Require employees and officers to sign a computer use policy. This policy should explain that information stored on government computers is not private; specify that computers should not be used for personal purposes, unless the policy allows for incidental personal use; and outline policies for misuse of equipment, subject to collective bargaining agreements.
- Monitor user access to the network.
- IT administration should use a web filter and review the logs it creates.
- Review audit logs of applications, including the financial software.
- When audit logs or other red flags indicate possible improper computer use, executive management should consider having IT administration review a sample of users' hard drives at unannounced intervals.
- Provide training to computer users on the use and protection of the IT assets related to the network.
- Monitor access to the network room. Secure the room with an alarm system. Install automatic fire-suppression in the network room.
- Backup sensitive data with encryption. Encrypt and/or password protect information that flows in and out of the system (through email or a portable device such as a data stick) or use portable devices that have password security.)
- Periodically restore backups.
- IDS systems are designed for extremely large networks. They're generally $10k+ and not infrequently require a staff to maintain regularly. Cannot be considered reasonable for your environment.