TECHNOLOGY COMMITTEE PROCEDURES

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 the director's computer.

Library Circulation System

- These files include all cataloging and circulation activities for the library's collection.
- These files are not maintained offsite.
- 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.

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. Patrons will not have individual accounts on each computer. The SAM security software offers them individual accounts but only tracks the account balance for printing. 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 When an employee leaves the Library, the system will be notified that their login is no longer valid.

Data Security

Segregate staff areas of the network from patron access from public computers and the WiFi.

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.

A password encryption program will be used to store and develop copies of the Library's passwords. The chair of the building committee shall have emergency access to this program and its contents.

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 available for use to the Director and a few select board members via a cloud product. The Director may also access the library circulation system offsite.
- 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, I think 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.

Items too Diffficult (or Costly) to Implement

- 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.
- Create a remote access policy. (Part of network security procedures.)
- Notifications for adding/removing users should be retained.
- Use an authentication system to log-on to the network and specific applications.
- Passwords should contain complexity requirements. (When possible, a password security program will be used.)
- Encourage users from writing down passwords.
- 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.
- Lock user accounts after three to seven consecutive attempts with an incorrect password.
- Lock user accounts after a certain period of inactivity.
- IT administration should give users access only to the areas of the applications and network they need to perform their job duties.
- IT administrations must ensure that default accounts for servers and applications are deleted, or at least that the passwords are changed.
- 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.
- Maintain a list that describes each time a backup was performed and the type of backup that took place.
- Backup sensitive data with encryption.
- Periodically restore backups.
- IDS systems are really only for extremely large networks. They're generally $10k+ and not infrequently require a staff to maintain regularly. Cannot be considered reasonable for your environment.
- If some or all of IT administration's duties are outsourced to a vendor, the contract with the vendor should provide that the vendor sign an authorization form agreeing to services to be provided and stating they will follow the local government's security policies: (From MHLS Staff): The MHLS contract with Sierra has certain provisions which are probably equal to any that might be required by a local government. We all work under certain best effort sort of clauses, but not necessarily anything specifically tied to local rules - nor does that seem particularly viable for the sorts of services and support we generally work with. I think this is really more targeted when you have a full time contractor onsite as the sole network administrator...as opposed to the role, say MHLS plays, which is at most administrative support to your own administrative actions. I'd say you're fine, but this is admittedly a trickier area.