COMPUTER & NETWORK SECURITY POLICY

USER ACCESS

All staff will be given a departmental login, which provides access to the computer and appropriate network drives.

Staff must respect the integrity and privacy of their coworkers' data accessible from communal network locations.

Authorized staff will be given login credentials to appropriate vendor/financial accounts. If the authorized staff is no longer a member of the library staff, the associate user account must have its password changed by the end of business day of the last day of employment.

Authorized IT staff will have access to administrative access to the local network and the remote Integrated Library System (ILS). If the authorized staff is no longer a member of the library staff, the associate user account must have its password changed by the end of business day of the last day of employment.

For information on email accounts, see the *Policy 500-210 Information and Communication Technology (ICT) Policy.*

PASSWORDS

Passwords subject to this policy:

- ILS
- Vendor accounts
- Financial accounts
- Payroll
- IT administrators

Passwords must be changed:

- Every 365 days
- Upon separation of an authorized staff member from the Library.

Password complexity requirements:

- At least 6 characters long
- Not contain any part of the user's name
- Not contain any information relating to the library (i.e 'library', 'connetquot', '11716', etc..)

Passwords must contain characters from two of the following four categories:

- Uppercase (A through Z)
- Lowercase (a through z)
- Numeral (0 through 9)
- Symbols (@, $)

REMOTE ACCESS

Local Network

- Approved staff may access the local network via SSL encrypted desktop protocol with authorization from Library Director (i.e. Network Administrators, IT consultant).

Offsite

- Approved staff may access various third party services via remote access if they are authorized and possess the proper credentials (i.e. email, payroll, website FTP, social media, etc..)

DATA PROTECTION/DISASTER RECOVERY

Local Network:

- Maintain UPS and surge protectors on servers.
- Server Room is locked and only accessible to authorized personnel.
- Server backups to external media are to occur weekly, after the end of business.
- Server backups to the cloud are to occur weekly, after the end of business.

Financial:

- Permissions to access to data are password protected.
- Backups to external media occur daily.
- Backups to cloud occur daily.

Firewall:

- Network is protected with an adaptive security appliance.
- Network is monitored by a third party provider.

Antivirus:

- Antivirus install on every applicable network device
- Core OS protection through restoring a computer back to its original configuration each time the computer restarts.
- DNS content filtering which blocks malware.

Integrated Library System:

- All patron and holdings data are stored offsite at the facilities of SirsiDynix.
- All application and data backups are stored in separate and secure locations.

Third-Party Data Storage (in addition to ILS)

All third-party vendors who store data on behalf of the Connetquot Public Library must have security measures in place which are in compliance to this policy and be vetted by our IT staff.

Examples of this include, but are not limited to:

- Payroll
- Cloud backups
- Website
- Digital Services

Policy 1000-10
Adopted 9/11/2014
Revised 11/10/2016