PERSONNEL
Information Technology (IT) Security

I. STATEMENT The Red Jacket Community Library (Library) outsources administration of the IT environment to the regional public library system, OWWL Library System (OWWL). Library employees must use computers and access software and data within the IT environment in performance of their duties.

II. PURPOSE To identify internal controls provided through OWWL, and to establish acceptable computer use criteria for the protection of Library IT resources.

III. POLICY

A. IT SERVICES AND ADMINISTRATION

1. OWWL oversees technical support, training, and resource sharing for the library and other sister libraries throughout the OWWL region.
2. OWWL provides centralized cataloging, coordinated technology purchasing, on-site library tech support, training for member libraries, and management of the shared integrated library system (ILS) and online catalog. The ILS comprises a relational database, software to interact with that database, and two graphical user interfaces (one for patrons and one for employees).
3. OWWL performs IT installation, monitoring, and maintenance of the wireless networks and provides virus protection, software patch management, active directory services, firewall updates and configurations, intrusion detection, back-up contingency planning, sanitation and disposal of hardware and electronic media, and website hosting.

B. EMPLOYEE COMPUTER ACCESS

1. The wireless access point is located at the circulation desk.
2. Each employee has access rights to an individual OWWL email account.
    a. The Director has access to another associated email address (redjacketlibrarydirector@owwl.org) with the username of “Library Director” as an email alias.
3. Each employee has access rights to an individual Evergreen account, managed by OWWL, with personal logins and passwords.
4. The Director is the only employee with administrative rights to the OWWL wireless network; other employees lack administrative rights and lack permission to download and install software.
5. After any employment separation occurs the Director shall notify OWWL whereupon the former employee’s network account shall be disabled within five days of separation.

6. A current list of authorized users shall be maintained by the Director.

C. NEW HARDWARE AND SOFTWARE

1. Orders for new hardware and software should normally be coordinated with OWWL.
2. Software additions or changes should be made by OWWL, when practical, to ensure the software works well with the network, is safe, and compatible for library use.
3. If software is installed by the Director, rather than OWWL, the Director must backup software by securing the master copies of the software with user instructions.

D. WEBSITE DOMAIN AND HOSTING

1. The public website, redjacket.owwl.org, is a sub-domain of OWWL.
    a. Any correspondence requesting domain renewals, website hosting, website directory listings or similar services must be reviewed by OWWL before considered for purchase.
2. OWWL maintains the web server with a dedicated WordPress install for the public website at no cost to the Library.
3. The Library is primarily responsible for WordPress updates and should perform them as soon as possible.
    a. OWWL may assist with plugin installation, but the Library is responsible for choosing and updating any WordPress plugins.
    b. The Library should limit the use of plugins, choose plugins that are actively supported and updated, and delete any plugins that are no longer needed.
4. OWWL has an administrator account and will run nightly backups, perform updates, debug issues, and monitor security status.
    a. The Director may appoint a web developer with administrator access to update the site.
    b. The Director may authorize other users to access the site as required for their work.
    c. Each user of the WordPress control panel must use their own login.

E. LOCAL IT SECURITY AND ACCEPTIBLE USE

1. User Account Security
    a. Employees are required to shut off computers during closing procedures.
    b. Laptops should be kept in a secure location when unattended; laptops should never be left unattended in a car or in public places including common areas within the library.
    c. All sensitive data should be stored on the network or in cloud-based files and not on computer hard drives.
2. Password Management Security
    a. Login profiles or passwords are required to access all computers designated for employee use; these include computers located at the circulation desk, the desktop

computer located in the Director's office, and laptop computers assigned to the Director, Treasurer, and full-time Clerk.

b. Passwords are required to access individual OWWL email accounts.
c. Personal passwords and profiles should never be shared with another person.
d. Password complexity requirements should be consistent with current advice from OWWL regarding password security.
e. Passwords should be changed when they are forgotten, upon indication of compromise, and consistent with current advice from OWWL regarding password security.
f. Passwords should not be written down or stored in an insecure manner.
g. Managing passwords that are required to access vendor accounts or official web portals are the responsibility of the officer accessing these accounts.

3. Restrictions on Personal Use

a. Connecting personally owned devices, including USB flash drives (sticks, thumb drives), to library computers is discouraged.
b. Personal software, even if for library use, should not be installed on a library computer.
c. Information stored on library computers is not private and library computers should not be used for personal purposes, except for incidental personal use.

F. IT SECURITY AWARENESS TRAINING

1. Annual Employee Training

a. At least one staff meeting each year should be designated for IT Security Awareness Training
b. Training shall be arranged or provided by the Director.

2. Training topics may include, but are not limited to the following:

a. Library IT assets, security risks, including computer access and acceptable use policy.
b. Recent or anticipated changes to hardware or software.
c. Password protection and access rights to files, documents, and applications.
d. Avoiding inadvertent download of potentially dangerous software or malware.
e. Copyright laws related to software licenses.
f. Expectations within job performance that support a secure IT environment.

3. Additional, intermittent, or ongoing IT security or computer training shall be offered to certain employees on an as needed basis at appropriate times, that include the following situations:

a. When new hardware, software, computer applications are installed or updated.
b. For new employees or changes in access rights of existing employees.

4. Training Acknowledgement

a. Employees, including Library officers, shall sign a computer use policy form (Appendix 1O) to acknowledge awareness training on the most current employee computer access and acceptable use policy.

b. The acknowledgement form will be kept in employee personnel folders; a copy will be provided to each employee.

G. COMPUTER INVENTORIES

1. Hardware Inventory

a. The Director shall maintain a comprehensive inventory for Library purchased computer hardware.
b. Inventory details should include the make, model, serial number, assigned users (if applicable), the physical location, and relevant purchase or lease information including the acquisition date for each asset.

2. Software Inventory

a. The Director shall maintain an inventory of authorized software installed on each Library computer. Inventory records should detail pertinent licensing information including the total number of licenses for each software, the computers on which each software is installed, and the number of copies of each software installed.
b. Only software necessary for Library operations shall be installed on employee computers.
c. The Library is responsible for the appropriate use of licensed software. For example, the Library may have purchased rights for a certain number of users, and it may be inappropriate or violate the license agreement to disseminate software to additional users.
d. The Director shall ensure that reviews of software installed on Library computers are performed at least once a year and that these results are compared to Library's software inventory records.

H. IT SECURITY POLICY MONITORING AND REVIEW

1. The Board of Trustees should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies and implementing internal controls.

IV. REFERENCES

Office of the New York State Comptroller. *Local Government Management Guide: Information Technology Governance.* Division of Local Government and School Accountability 110 State Street, Albany, New York 12236, 2021, https://www.osc.state.ny.us/files/local-government/publications/pdf/information-technology-governance.pdf; accessed 3 November 2022.

Federal Communications Commission. *Children's Internet Protection Act (CIPA)*. Consumer and Governmental Affairs Bureau 45 L Street NE, Washington, DC 20554, 2019, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act; accessed 3 November 2022.

Revision History	
4/17/2023	Changed Pioneer Library References to OWWL. Removed reference associated with Red Jacket Schools and WFL BOCES. Updated changes to employee account access and annual training. Reformatted in accordance with Policy 100-2.