PERSONNEL
Information Technology (IT) Security

STATEMENT: The Red Jacket Community Library outsources administration of the IT environment to a service organization, Pioneer Library System (PLS). As third-party specialists, PLS staff provide IT services through intermunicipal cooperation with other regional libraries.

In addition, the Red Jacket Community Library is a shared-use facility with the Red Jacket Elementary Library and the Red Jacket HS/MS Library and receives library automation services as a cooperative service via Wayne-Finger Lakes BOCES (W-FL BOCES) School Library System (SLS).

Library employees must access software and data within the IT environment in performance of their duties.

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

POLICY:

IT SERVICES AND ADMINISTRATION

1. PLS oversees technical support, training, and resource sharing for the Red Jacket Community Library and other sister libraries throughout the PLS region.
2. The PLS technology staff provides centralized cataloging, coordinated technology purchasing, on-site library tech support, training to member library staff, 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 staff).
3. The PLS technology staff performs IT installation, monitoring, and maintenance of the following:
    A. Wireless Networks
    B. Virus Protection, Software Patch Management, and Active Directory Services
    C. Firewall Updates and Configurations and Intrusion Detection
    D. Back-up Contingency Planning
    E. Sanitation and Disposal of Hardware and Electronic Media
    F. Website Hosting
4. The SLS staff provides software system upgrades and support for circulation, cataloging, and reports for school-owned materials.
5. Employee Computer Access
    A. Wireless Access Point
        - The access point is located at the circulation desk. It should be turned on each day when the library opens and should be turned off when the library closes.
    B. Access Rights
        - Each employee has access rights to a personal PLS email account.
        - Employees share two user accounts on computers installed with Evergreen (managed by PLS) and Mandarin (managed by WFL BOCES).
        - The Director has access to a personal PLS network account and email account and is the only employee with administrative rights; other employees lack administrative rights and do not have permission to download and install software.
        - The Director also has access to one-generic email account (redjacketlibrarydirector@owwl.org) with a user name of “Library Director”.
    C. Access Control
        - After any employment separation occurs the Director shall notify PLS technology staff whereupon the former employee’s network account shall be disabled within five days of separation.
        - A current list of authorized users shall be maintained by the Director.
    D. New Hardware and Software
        - Orders for new hardware and software should normally be coordinated with PLS IT staff.

- Software additions or changes should be made by PLS IT staff, when practical, to ensure the software works well with the network, is safe to use, and is for business use. If software is installed at the library, and not by PLS, the Director should backup software by securing the master copies of the software and its user instructions.

E. Website Domain and Hosting
- The public website, redjacket.owwl.org, is a sub-domain of Pioneer Library System. PLS maintains the domain at no cost to RJCL. Any correspondence requesting domain renewals, website hosting, website directory listings or similar services should be reviewed with PLS.
- PLS maintains the web server with a dedicated WordPress install for the RJCL website at no cost to RJCL. The Library is primarily responsible for WordPress updates and should perform them as soon as possible. The Library is responsible for choosing and updating any WordPress plugins. PLS may assist with plugin installation. 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.
- Each authorized user of the WordPress control panel must use their own login.
- PLS has an administrator account (plsadmin) and will run nightly backups, perform updates, debug issues and monitor security status.
- The Library Director (redjacketlibrarydirector@owwl.org) has an administrator account. The Director may appoint a web developer with administrator access to update the site. The Director may authorize other users to access the site as required for their work.

<u>LOCAL IT SECURITY</u>

1. Acceptable Use
   A. User Account Security
      - Employees are required to shut off computers during closing procedures.
      - 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.
      - All sensitive data should be stored on the network or in cloud-based files and not on computer hard drives.

   B. Password Management Security
      - 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, Youth Librarian, and the Treasurer.
      - Passwords are required to access personal PLS email accounts.
      - Personal passwords and profiles should never be shared with another person.
      - Password complexity requirements should be consistent with current PLS advice regarding password security.
      - Passwords should be changed when they are forgotten, upon indication of compromise, and consistent with current PLS advice regarding password security.
      - Passwords should not be written down or stored in an insecure manner.
      - Managing passwords that are required to access vendor accounts or official web portals are the responsibility of the officer accessing these accounts.

   C. Restrictions on Personal Use
      - Connecting personally owned devices, including USB cables, to library computers is discouraged.
      - Personal software, even if for a library use, should not be installed on a library computer.
      - Information stored on library computers is not private and library computers should not be used for personal purposes, except for incidental personal use.

2. IT Security Awareness Training
   A. Annual Training for Employees
      - At least one staff meeting each year should be designated for IT Security Awareness Training
      - Training shall be arranged or provided by the Director and include topics related to:
        - Library's IT assets and security risks including computer access and acceptable use policy.
        - Recent or anticipated changes to hardware or software.
        - Password protection and access rights to files, documents, and applications.
        - Avoiding inadvertent download of potentially dangerous software or malware.
        - Copyright laws related to software licenses.

- Expectations within job performance that support a secure IT environment.

B. Additional Security or Computer Training
- Additional IT security or computer training shall be offered to certain employees on an as needed basis at appropriate times, that include the following situations:
  - When new hardware, software, computer applications are installed or updated.
  - For new employees or changes in access rights of existing employees.

C. Employees, including library officers, shall sign a computer use policy form to acknowledge awareness training on the most current employee computer access and acceptable use policy.

3. Computer Inventories

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

B. Software Inventory
- 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.
- Only software necessary for library operations shall be installed on employee computers.
- Employee access to licensed software shall be accessible only by appropriate users - those who need it to perform their duties. The library is responsible for the appropriate use of licensed software. For example, the library may have purchased rights for only a certain number of users, and it may be inappropriate or violate the license agreement to disseminate software to additional users.
- 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.

IT SECURITY POLICY MONITORING AND REVIEW

The Board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.