MVLS/SALS Joint Automation Project
Amendment to JA Security Policy
November 8, 2017

Statement

The JA Council oversees and administers the automation project used by 58 libraries in eight counties. The MVLS/SALS Joint Automation Council approved a JA Information Security Policy, January 11, 2017, SALS Board of Trustees on January 17, 2017 and MVLS Board of Trustees on January 19, 2017. This policy addresses acceptable use, passwords, email, remote access, confidentiality of library patron data, and confidential personnel data.

Section V. Confidential Library Patron Data Policy, sections 4.2-4.6

Regulations

1. Only the library director may request patron data from either the MVLS or SALS system trainers.
2. The data may be used to send out newsletters, budget mailings, the library's long-range plan, and annual report to the community and for other internal uses.
3. The data cannot be used for Vote Yes campaigns or library fundraisers. The Friends of the Library or other groups cannot have access to the data.
4. ~~The data must be encrypted in transmission and storage amongst MVLS/SALS users on computers within the SALS/MVLS network, not on home or private computers.~~ The data must be encrypted in transmission and storage and only accessed by authorized users. The data should never be accessed or stored on ~~home or private computers.~~ non-JA approved devices (i.e., home computers, personal iPads, cell phones).
5. The Polaris data file provided by JA must be deleted after each specific use.
6. A library may develop and maintain its own mailing/contact list that may contain email address, phone number or mailing address. When MVLS/SALS Joint Automation Project data is used as a source for this separate database, the library must inform the patron that they are part of the mailing list and give the patron the option of opting off the list. It is the library's responsibility to keep this list confidential and develop an internal policy regarding the list and to tell patrons on the list of the potential uses of the list. If the information is used for direct contact to specific patrons, the patrons should be notified in advance that is a possibility and given the option to opt out. If a library uses a third party to manage this separate database (Constant Contact, etc.):
    a. The data must be transmitted to the third party in encrypted form
    b. There must be a written agreement with the third party as detailed in section 4.5 on page 36 (covering responsibility, security, transmission and disposal)

Approved Joint Automation Council 11/8/2017
Approved MVLS Board of Trustees 11/16/2017
Approved SALS Board of Trustees 11/21/2017

MVLS/SALS Joint Automation
Security Description

Summary

The Mohawk Valley Library System and the Southern Adirondack Library System have jointly provided integrated automation services to their member libraries since 1983 through the MVLS/SALS Joint Automation Project.

The MVLS/SALS Joint Automation Project is a cooperative project, sharing resources in eight counties served by the two library systems. As part of the MVLS/SALS Joint Automation Project, each library works collaboratively with other member libraries, the Joint Automation Council, Joint Automation Staff and system staff to insure the efficient operation and security of the automated system for all participants.

With a shared patron database, each library is expected to enforce confidentiality laws and policies to insure that all personal information including borrowing, requests, and information searches remain private. The Joint Automation Project takes very seriously its responsibility to respect the privacy of every user and expects libraries to enact appropriate local policies, procedures, and necessary training to protect confidentiality.

This document outlines security policies and procedures that are employed by the Joint Automation staff and are required of the users of the MVLS/SALS integrated automation services. The Board President from each library annually signs a memo of understanding stating that they understand and will fulfill the following policies and procedures.

Policies and Procedures

Staff user accounts and staff responsibilities

- All users are responsible for maintaining the security and privacy of all Polaris data and all patron information
- Social Security numbers are never recorded in Polaris (see *Patron Social Security Policy*)
- All users will have the least amount of access and/or permissions necessary to do their job
- Access to Polaris (where patron data is stored) is granted based on staff person and device
- ~~Any~~ users of the MVLS/SALS email system are only allowed to use the encrypted web-based interface ~~provided~~, installed Outlook on a PC, or Outlook app on portable devices
- User accounts for staff who are no longer employed by the library are removed within 30 days of when the person leaves library employment
- Passwords
    - All users are responsible for maintaining the security of all passwords
        - Passwords are never written down
        - Passwords are never shared with anyone
    - Strict password requirements are enforced for all users
        - Passwords have to be unique and complex and expire regularly
        - Break-in evasion policies are in place that prevent devices / accounts from logging on after bad attempts

MVLS/SALS Joint Automation
Security Description

Protecting Data

- Any data in the Polaris system that identifies a specific patron in a transaction (check out, hold request etc.) is cleared from the database after 31 days, unless needed to conduct business
- Offline files can only be installed on authorized staff PCs on the staff network
- SSL encryption is used for patron functions of the PAC and all external authentication (i.e. Cassie, Overdrive)
- Credit cards
    - Credit cards are not ever handled by staff if the library accepts credit card payments via self-check or Comprise payment terminal on a staff workstation
    - Credit cards are only handled by staff when the library has a credit card terminal at the circulation desk connected directly to the merchant bank
    - When credit cards are handled by authorized staff
        - Cards are never copied
        - Full credit card numbers are not displayed on receipts
        - Printed receipts are stored in a safe area
        - Printed receipts are destroyed when they are over a certain age
    - Accepting Credit Cards in the Polaris PAC
        - Credit card payments in the PAC are designed to be recorded from the patron's home computers (the credit card number entry is not masked)
        - For PAC computers on the MVLS/SALS network, the PAC computers are added to "in house" workstations so that the payment option is not available (patrons are not allowed to make credit card payments from PACs on the staff network)
- Library records, as defined by NYS law 4509, are not released or made available in any format to a federal agent, law enforcement officer or other person unless a court of competent jurisdiction has entered a court order in proper form (see *Disclosure of library records policy*)

Server Administration

- Current antivirus software is maintained on all servers, including real-time scanning and daily definition updates
- There is up-to-date patching of all servers, within 30 days of release
- Backups
    - All domain controllers are backed up daily (including the System State)
    - Each daily backup save set will be retained for at least 1 week
    - The backup from the previous day will be stored off site for 1 day
- The MVLS/SALS data center is locked at all times with access only to necessary system and automation staff
- There is minimal administrator access to all servers
- Server event logs are monitored on a regular basis

Network Requirements

- MVLS/SALS maintains a firewall for the protection of the servers located at the MVLS/SALS data center

- MVLS/SALS maintains IDS/IPS (intrusion detection/prevention) at the MVLS/SALS data center – this provides monitoring and prevention of unauthorized access to the network and servers
- All member library sites are protected with firewalls and routing rules to prevent unauthorized access (see *Network Connections policy)*
- Staff, public and wireless networks are always separate (see *Wireless Network policy)*
- Techniques are used on wired networks to prevent unauthorized devices from being connected
- Only network drops that are in use are patched to the network backbone switches
- Wireless access to staff or public wired networks is not allowed
- Credit card devices used on self-checks and/or staff workstations must be on a separate isolated network, and must be inaccessible from the staff network and from outside the network
- All network configurations are documented
- ~~Staff network drops are subject to regular (minimum every 3 months) surveys~~
- ~~The staff network is~~ Authorized staff will regularly inspect~~ed~~ for unauthorized wireless networks and audit network drops
- External access to the staff network is only allowed via VPN

PC Requirements

- All PCs are required to have virus protection, including real-time scanning and daily definition updates
- All PCs are required to be running current, updated and fully patched operating systems
- All devices connected to the staff and public networks must meet the minimum requirements set forth by the automation staff (see *Workstation Purchase and Support policy*)

Equipment Disposal

- When PCs are retired all hard drives are securely erased or destroyed prior to disposal or reuse (see *Equipment Disposal policy*)