MVLS/SALS Joint Automation Project
Amendment to JA Security Policy
Approved 6/18/2024

Proposed May 14, 2025

Statement
The JA Council oversees and administers the automation project used by participating libraries in the Mohawk Valley and the Southern Adirondack Library Systems ~~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 and only accessed by authorized users. The data should never be accessed or stored on 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)

Revision approved SALS Board 6/18/2024