MVLS/SALS Security Policy FAQ
Proposed May 14, 2025

Why are the Mohawk Valley Library System (MVLS), the Southern Adirondack Library System (SALS) and the Joint Automation Council (JA) requiring member library staff and volunteers agree to and sign the Information Security Policy?

JA serves participating libraries in the Mohawk Valley and the Southern Adirondack Library Systems. ~~There are forty-eight public libraries located in the eight county region.~~ Inappropriate use, whether accidental or intended exposes MVLS, SALS and the member libraries to risk. The purpose of this policy is to detail the acceptable use of POLARIS, the network, the internet and the staff computer workstations for the protection the two systems and all of the member libraries.

Who reviewed the draft of the Information Security Policy?

The Information Security Policy was reviewed by the JA policy committee (Michele Largeteau, Diane Robinson, Sara Dallas, Eric Trahan, Devon Hedges, Ike Pulver) and shared with the full JA Council (K. Naftaly, E. Wing, E. Trahan, S. Dallas, J. Borrelli, R. Wise, T, McDonough, K. Kakeh, M. Largeteau, K. Bradley, D. Hedges.

Who needs to approve the Information Security Policy?

The JA Council will vote to accept the policy. The MVLS Board of Trustees and the SALS Board of Trustees will need to approve the policy.

Will there be a summary document to explain the MVLS/SALS Joint Automation Project Information Security Policy?

Yes, there are one page summaries to highlight the guidelines. The summaries available are:

Acceptable Use Policy
Password Policy
Email Policy
Confidential Library Patron Data Policy

Will there be an informational or training session available to explain the MVLS/SALS Joint Automation Project Information Security Policy to the directors?

Yes there will be informational meetings to explain the full document. System and JA staff are also available to explain the document as needed.

Some training tools will be developed.

Who is required to sign the MVLS/SALS Joint Automation Project Information Security Policy?

Employees and volunteers do not need to sign all parts of the policy. It depends upon their responsibilities.

Everyone who uses a **staff computer workstation** will need to sign the **Acceptable Use section**.

Everyone who has a **password** for any staff or public computer, Polaris account or MVLS/SALS Email account will need to sign the **Password section**.

Everyone who has an mvls.info or sals.edu email address will need to sign the **Email Policy section** of the MVLS/SALS Joint Automation Project Information Security Policy.

Everyone who has access to the **POLARIS database** will need to sign **the confidentiality data section**.

Anyone who has access to **Confidential Personnel and Financial data**, will need to sign to the **Confidential Personnel and Financial data section** of the policy.

Remote access is only for technical/computer/network staff at some member libraries, JA staff and SALS staff.

Some library staff and/or volunteers do check in and out and check their email and that's really the extent of their computer skills. Do they need to sign the entire policy?

Library staff and/or volunteers will need to sign parts of the policy that apply to their responsibilities. For example, a staff/volunteer who has access to the POLARIS database and checks library materials out or in, will need to sign the Acceptable Use, Password and Confidential library patron data sections of the policy.

If the staff/volunteer uses a staff workstation to check his/her email they would have to sign Acceptable use, password and Email sections of the security policy.

Can a library employee expect privacy in their email account?

Emails that end with mvls.info or sals.edu are work emails. Employees should have no expectation that their work emails are private. Joint automation staff will not read the emails. However if a library board or a library director requests access to these accounts, access will be given. In addition, if MVLS or SALS is issued a subpoena or warrant, the information will be shared as indicated by the legal document.

What is Peer-to-Peer (P2P) file sharing?

Distribution and sharing of digital files (could be music or movies or other content) using peer-to-peer (P2P) networking technology. Peer to peer network technology is when members / users of a software application search for connected computers on the network to locate files they are interested in getting and then the files are transferred directly from one member computer to another (without an intermediary). Usually the files are large in size so the file transfer can have an impact on network performance.

Sometimes the files that people want to receive on P2P networks are copyright protected (e.g. music or movies) and sharing them would be illegal.

To avoid:

- Don't install software that advertises accessibility to free digital content that you know is copyrighted
- Don't copy movies or music to staff PCs
- When in doubt, discuss with JA staff

Some examples of P2P file sharing are: LimeWire, Napster, Guntella, and Kazza. Avoid anything with the word "torrent" in the name.

Can we still use Google Docs or Dropbox?

Yes.

Can we still use an USB stick on a work computer?

Yes, use of an USB stick is still allowed. However, care needs to be taken when using the USB. The stick must be from a trusted source. Never insert an USB stick given to you by a member of the public into a staff computer. Up to date Antivirus software must be installed on all staff computer workstations.

How can I monitor bandwidth?

There are some programs and streaming videos that use a great deal of bandwidth. Please call JA and ask for assistance.

MVLS/SALS Security Policy FAQ
Proposed May 14, 2025

How would I know someone is using a great deal of bandwidth?

People will complain that the response is slow or some libraries will notice their circulation functions slowing down.

What is considered a reasonable size for attachments?

25 MB or higher is the cut off limit for attachments. If you are not sure how to determine the size of an attachment, please contact JA.

Do we need to tell people no hacking?

Yes, there needs to be a policy statement to protect your library, MVLS and SALS.

Are the overdue notices and bills that contain information about the patron (address, phone number, and reading history) confidential? Do they require a signature?

Yes, if the overdue notices and bills are confidential. The overdue notices and bills contain the name of the library and a disclaimer statement

The library's printer or fax machine is not in a secure part of the library. Does it need to be moved?

The printer used by the public can be in a public area. The printer used by the library staff to print confidential information cannot be in the public area.

Several areas say to store information in encrypted form. How do I do that? When?

The JA staff will be rolling out a new email system shortly. JA staff will be sharing information on how to encrypt individual messages. For more clarification, please contact JA.

If a staff member is out for any reason, can the director or supervisor check the work email account?

Yes, consider the email account an extension of a workspace. In addition, the computer workstation is also an extension of the workspace. Consider it a desk drawer or file cabinet.

MVLS/SALS Security Policy FAQ
Proposed May 14, 2025

Does this policy apply to the public use computers?

No. This policy applies to people with access to POLARIS and have an mvls.info or sals.edu email address.

All staff and volunteers should follow the Password policy for any public PC passwords.

Encryption of email - Is this something that is set up for the entire email system by JA or are there other steps that staff need to take when sending email?

JA staff is working to address this issue. It will be available very shortly.

Do email disclaimers need to be attached to ALL email sent?

Yes– This is added automatically when using an mvls.info or sals.edu address

I would like to update our procedures to comply with the new JA policy. Can we work on this together?

Of course, please contact someone at your system (MVLS or SALS).

What if the library policy is more secure than this one?

Use and enforce the more stringent policy. Please share a copy of your policy with the JA staff.

What if an employee or volunteer refuses to sign the appropriate parts of the policy?

The employee or volunteer will no longer have access to their email or POLARIS or computer workstation.

Can the public use a staff workstation?

No.

MVLS/SALS Security Policy FAQ
Proposed May 14, 2025

Is it ok to use slips that contain the full patron name and the item title on self-pickup hold shelves (which by definition are never in a secured area?)

This is a policy that is locally decided. Patron must be given the option to opt out and have their items held in a more secure area.

Is it ok to use slips that contain the full patron name and the item title in the delivery?

Every effort should be made to remove the slips when returning the library materials to the owning library.