User Account Policy

Proposed 5/14/2024

Access to the MVLS/SALS Polaris database, email, OneDrive and Microsoft Office 365 is provided based on the level of access needed for library staff to do their jobs. **For the best security, it is essential that all users are trained, access is never given at a level higher than needed, and access is removed when staff leave.**

In order to maintain this level of secure access, the following policies must be followed for user account access:

- Users should never, under any circumstances, share usernames and passwords, or allow another user to use their account.
- An MVLS/SALS email account is required for all users. Users must monitor this account regularly. Email from an MVLS/SALS email account cannot be automatically/blanketly forwarded to any external email service.
- Multi-factor authentication (MFA) is required for all user accounts.
- All users must sign the MVLS/SALS Joint Automation Security Policy annually or their account will expire.
    - When their account expires – Polaris, email, OneDrive and all Microsoft Office 365 access is automatically disabled.
- All users must complete assigned phishing and security trainings, or their access to Polaris, email, OneDrive and Microsoft Office 365 will be disabled.
- When a staff person is no longer working for a library or their job function changes, the library must inform JA immediately.
    - It is very important to disable access when a staff person retires, resigns or is no longer employed by a library for any reason.
    - If a library needs to retain access to email or OneDrive files for a temporary period of time, there are ways to set that up while still protecting the security of the system.
    - If a staff member takes an extended leave (maternity, seasonal, retiring but not off the books yet, etc.), JA must be notified so that the Polaris account can be suspended for security. Keeping email in these situations is ok, but Polaris access must be suspended when it is not needed.
    - If an employee changes positions, their Polaris permissions should be reassessed.
- All Polaris account requests (new users, change of Polaris permissions) will go through the system trainers.
    - Polaris permissions are based on job function, not job title.
    - Users must be trained for Polaris access (either by the system trainers or library staff as approved by the system trainers).
    - For complex Polaris functions, only staff who will be performing those functions regularly will be given access.
- If a user's account is expired for more 3 months, JA will contact the library director about removing the account from the system.
- If a user has not logged into Polaris in more than 3 months, Polaris access will be suspended and JA will contact the library director about removing the account.

User Account Policy

Proposed 5/14/2024

- For libraries that want to keep a substitute list for very occasional work:
    - If they have not signed the security policy and their account expires, JA will need to be contacted to re-activate the account, and they will need to sign the security policy at that time before access is restored.
        - System trainers will determine if training is required before Polaris access is given.
    - These users must complete assigned phishing and security trainings when assigned, or their access to Polaris, email, OneDrive and Microsoft Office 365 will be disabled.

Revision approved JA Council 5/8/2024
Revision approved MVLS Board 5/16/2024
Revision approved SALS Board 6/18/2024