HELEN PLUM LIBRARY

U-11 IT Security
Approved by the Library Board of Trustees April 8, 2014.
Reviewed by the Library Board of Trustees July 19, 2022.

Objective of the Policy

The purpose of this policy is to safeguard Library data and IT resources so that Library patrons trust the Library to protect their information and to serve as effective stewards of public funds invested in the Library's IT resources.

Principles

The most valuable Library IT resources are the Library's IT staff followed closely by the data the Library maintains. The Library's IT network must be secure to protect patron privacy and to ensure bandwidth is available for staff use for Library business and for patron use.

Responsibilities

The Library's IT Department is charged with the responsibility to provide a secure Library network with sufficient safeguards such that the network is available for Library use and protects patron data. This includes establishing and following Library IT Guidelines and best practices for network access security, use of Library IT equipment, data backup and recovery plans.

All Library staff members are responsible for following the aforementioned Library IT Guidelines established by the IT Department. Patrons are responsible for following the Internet Use Policy established by the Library Board.

Network Access

Library equipment should be used to access the Library network whenever practical because it is configured so as to be secure. Logins and passwords established to make equipment and network access secure should be provided with sufficient authorizations to enable staff to do their jobs, yet prevent access to data, functions, and resources not required for a staff member's responsibilities. This is true for network access from within the building as well as from any off-site location. These logins and passwords should be changed on a recurring schedule in relationship to staff turnover. The IT staff should change passwords as their best judgment dictates.

Vendors should only be granted access to the portion of the Library network they support. Ideally this should be provided only when IT staff is present and only for the duration of a support session, e.g., with such products as TeamViewer that provides a single session access that requires a per session code. Default passwords provided by vendors should be changed as soon as practical.

Passwords within the Library network can be reset by IT Staff to allow access in the event of unforeseen circumstances. Each department head is responsible for maintaining a secure list of logins and passwords used by her/his department to conduct Library business with external vendors. She/he is responsible for informing the Library Director where/how the list could be accessed.

Personal devices owned by Library staff should only be used to access Library email and the Library network when they meet the minimum-security requirements established by the IT Department. These are not enumerated here, as they will always be evolving. They should include password and anti-

malware protection whenever applicable. The IT Department should review and update these requirements that are to be included in the Library IT Guidelines at least annually with the Library Director. Any changes should be communicated to all Library staff and the IT Department should help staff determine how to remain in compliance with these minimal requirements.

All Library employees and Trustees should be aware that anything related to Library business, whether it uses the Library network or not, whether it is conducted using Library equipment or personal devices, is subject to the Open Meetings and Freedom of Information Acts and can become discoverable in any legal actions pursued.

Data

The best way to safeguard confidential information is to retain only the types of data required for Library business for as long as is required to conduct Library business or to meet any legal data retention requirements. For example, the Library has no need of patron social security numbers so should not request or store that information. The Circulation Department has the responsibility to determine the intervals for which patron checkout and billing histories should be kept with a goal of keeping them no longer than required to conduct Library business. Per the Library Board's Privacy Policy, U-4, all Library staff members are to safeguard patron data; they should not view patron information or discuss it with other staff members unless it is required for Library business.

To minimize the risk of stored data being compromised, data should be stored on the Library's servers rather than individual computers or devices. In particular, no patron data that is exported from our integrated library system (ILS) server, for whatever reason, and no private Library personnel information should be stored on staff member's computers, Library laptops, or USB drives, unless it is encrypted. Any encryption technology used by staff must be approved by the Library's IT Department. Server backups, when taken off-site for disaster recovery purposes, should also be encrypted if recovery software can accommodate this. To safeguard data in transmission, staff IT equipment should use the Library's Local Area Network or the Library's staff wireless network rather than the Library's public wireless network. In addition, any personal devices used to access Library data, including email, should use either the Library's staff wireless network or the staff member's wireless carrier's cellular network, rather than the Library's public wireless network.

Library IT Equipment Usage

To ensure that Library IT equipment and network bandwidth are available for Library business, Library staff should refrain from downloading or installing personal software and media on Library equipment. Library email should be used for Library purposes. It is permissible to use the Library network to access the Internet for personal use on breaks, but this should always be done in such a way as to be non-interfering with Library business and consistent with Copyright Laws (for software, eBooks, music, etc.).