AVON
FREE PUBLIC LIBRARY

Cybersecurity Policy

Purpose:

This policy serves as a guide for the librarians and staff of the Avon Free Public Library (the "Library") in the use of technology assets and equipment so that the Library, staff and patrons may be protected from the repercussions of unauthorized access to library data or systems.

Key Definitions:

Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data or the measures taken to achieve the purpose of this policy.

Malware is software that is specifically designed to disrupt, damage or gain unauthorized access to a computer system.

Technology assets are all computing, networking and software applications that can be accessed by Users.

Users are anyone who has authorized access to Library computer assets through any technological equipment, whether owned or leased by the Library, or owned or leased by a third party. This shall include full time, temporary and part time employees.

Scope:

This policy applies to all employees of the Library, including full time, part time and temporary employees. This Policy does not cover topics addressed in the Social Media and Privacy policies.

Roles and Responsibilities:

Technology and Technical Services Staff are responsible for procuring, installing and maintaining Library technology assets and allowing access to the assets. They are also responsible for creating and maintaining cybersecurity protections for Library assets and data.

The Library Director is responsible for enforcing the Cybersecurity Policy and ensuring that adequate resources are available to execute the policy.

Library staff are responsible for understanding and following the procedures documented in the policy.

Library staff Procedures:

- Staff with computer access should use individual, unique accounts with the exception of the computers used at the service desks.
- Staff should not disclose their password to any other person.
- Staff with domain administrator access should use separate accounts for administrative tasks than their normal user access.
- Staff should not download software or modify the configuration of any computer without the direction and approval of the Technology and Technical Services staff.
- Staff with Library email access should avoid opening or acting on suspicious emails.
- Staff leaving their desk should lock the screen to prevent others from accessing the computer. Staff leaving for the day should logoff the computer.
- Staff should use Library computers, email and internet access primarily for Library business.

Technology and Technical Services Procedures:

Backup and Recovery:

- Maintain off-site backups of key Library files.
- Document a recovery playbook to recover data in the event of a loss.
- Practice a recovery at least once a year.

Network:

- Maintain a firewall for incoming traffic.
- Have a procedure and capability for block listing and allow listing of internet sites.
- Implement network segmentation of public computers and staff computers.

Maintain technology assets:

- Document an inventory list of all hardware and software.
- Remediate hardware and software vulnerabilities in a timely manner, prioritizing critical and high vulnerabilities.
- Maintain anti-virus and anti-malware on individual computers.
- Computers or other devices capable of holding data should be wiped prior to disposal.

User Accounts:

- Require users to create strong passwords by enforcing a password policy, including lockouts after a specified number of failures.
- Implement time-outs on network login and display lock after a specified time.
- Disable user accounts on the network, software and computer login when staff leave the employment of the Library.
- Use multi-factor authentication where appropriate.

Hardware:

- Library workstations should be configured to automatically scan removable media, when inserted, for malware, and to prevent executable files on external drives from being executed.

Enforcement and Appeal Process:

Library staff may be exempted from any of these restrictions if their scope of work requires that they perform the restricted activity in question. Prior to performing the activity, the staff member should request permission from the Library Director and the Technology and Technical Services Manager. Staff usage of technology assets may be monitored, removed or curtailed based on inappropriate, damaging or detrimental usage or because of other violations of this policy as determined by the Library Director.

Other Applicable Policies:

Internet Use Policy

Privacy Policy

Social Media Policy

Location:

This policy is housed on the Avon Free Public Library website: https://www.avonctlibrary.info/policies/

A copy is maintained in the Administration Office

Adopted: June 20, 2023