Policy: # 900-3
Adopted Date: [Pending Board Adoption]
Revised Date: N/A

Policy on Cybersecurity

Purpose

This policy covers all electronic information resources in the library. It applies equally to network servers, workstations, both staff and public access, network equipment, telecommunications equipment, and peripherals, such as printers, within the library.

Scope and Applicability

The policy applies to all library staff, volunteers, patrons, and contract workers using the library's computer resources. The library will take every reasonable precaution to ensure that any confidential information that is kept by the library for any purpose is safeguarded from unauthorized access. Within the credit card holder data environment, the library will also comply with the latest revision of the Payment Card Industry Data Security Standards (PCI DSS).

Cybersecurity Responsibility

The Library Director is responsible for overseeing cybersecurity and the development of the Cybersecurity Program. The Library Director may designate an Information Systems Manager (ISM) to assist in this responsibility.

The Information Systems Manager must ensure that the following standards are met on every computing system, equipment, or network with access to confidential information:

- Maintain an inventory of all computing assets, including hardware and software
- Secure computing systems, equipment, and networks with confidential information
- Restrict physical and login access to authorized users
- Maintain up-to-date software patches and anti-virus software
- Ensure and maintain complete system backups; backups should be redundant, both on-site and off-site.
- Enable and use host-based firewalls if available
- Perform regular security scans on computing systems, equipment, and networks

- Provide training, or at least written training materials, to all staff, volunteers, and contract workers detailing the appropriate use of the network, awareness of the possible effects of misuse or unauthorized use of computer resources, and the consequences of any unauthorized use. This should be provided at the time of allowing access and at least annually.

Policy Review

This security policy must be reviewed at least once per year and updated as needed to maintain alignment with applicable regulatory, audit, and National Institute of Standards and Technology (NIST) cybersecurity framework requirements.

Separate Systems

Computers responsible for internal processes will be kept on a separate network from patron-facing computers.

Password Management

Employee passwords must be kept secure. Sharing passwords is forbidden. Access to critical systems will require two-factor identification. User passwords must be changed if there is reason to believe they may have been compromised, but they will not expire on a time schedule. Use of a "Password Safe" or "Password Manager" is recommended.

Anti-Malware Protection

Anti-malware (antivirus) software must be installed, enabled, and active on all computers and devices. Exceptions for specialized devices must be documented and mitigated through equivalent controls.

Incident Response and Contingency Plan

An incident response and contingency plan must be maintained, reviewed, and updated annually or after major incidents. The plan must be tested through tabletop exercises at least once per year and retained in both digital and printed forms. Cybersecurity program documents, incident reports, and security procurement records (including hardware/software details and vendor names) are not public records.

The use of removable media such as USB drives should be prohibited on critical systems and discouraged for patrons unless such devices have been vetted and approved by the ISM.

Breach of Security

Any actual or suspected security breaches involving confidential information must be reported immediately to the Information Systems Manager and the Director. Incident response procedures will be initiated to identify the suspected breach, remediate the breach, and notify appropriate parties.

Adopted: [Date of Board Adoption]
Revised: N/A
Reviewed: