Cybersecurity Policy

In an era where cyberattacks are becoming more frequent and sophisticated, the 5 C's of cybersecurity—Change, Compliance, Cost, Continuity, and Coverage—offer a comprehensive framework for businesses to safeguard their operations.

Cybersecurity is a broad term. It refers to the activities, practices, and technology that keep computers, networks, programs, and data secure and protected from harmful activities such as unauthorized access, modification, or damage. Cybersecurity is defined as the administrative, technical, or physical safeguards the Lone Cone Library uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle confidential customer or staff information.

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.

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. The policy applies to all Library staff, volunteers, and contract workers using the Library's computer resources.

It is the intention of the Board of Trustees of the Lone Cone Library to maintain a solid program of network security and to review this policy annually, in order to accomplish the following:

1. Analyze the risks associated with threats to network resources
2. Determine which risks are most likely to occur-It's not a factor of "if," but "when."
3. Apply current practice in protecting against these risks, while maintaining functionality
4. Review security alerts and bulletins regularly for the emergence of new vulnerabilities

ALA GUIDELINES– The Lone Cone Library adheres to the policies set forth by the American Library Association regarding privacy guidelines and the intelligent use of technology.

Last date approved: 11/16/2026
Approved by: Lone Cone Library Board of Trustees on 11/17/2025

ROLES AND RESPONSIBILITIES

The Library Director will be designated to oversee the library's information security program. They will address potential risks to the security, confidentiality, and integrity of confidential information that could result in a compromise. They must ensure that the following standards are met on every computing system, equipment, or network with access to confidential information:

- 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
- 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 in 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.

Authorized Users

Authorized users may be staff members, volunteers, and contract workers. They are responsible for confidential information in their custody. Maintaining the confidentiality, integrity, availability, and regulatory compliance of confidential information stored, processed, or transmitted at the library is a requirement of all authorized users. All authorized users with access to confidential information will:

- Be assigned a unique user ID and initial password according to established procedure to gain access to network resources. Users must not share or disclose unique user IDs/passwords unless the user ID is already designated as a departmental "shared" user ID/password.

- Notify their manager immediately if confidential information, passwords, or other system access control mechanisms are lost, stolen, or disclosed or suspected of being lost, stolen, or disclosed.
- Restrict physical access to laptop computers when the user is physically away from it by keeping the laptop locked away when not in immediate use.
- Secure all staff computers by using a screen saver or built-in lock feature when the user physically walks away from the workspace.
- Maintain possession or control of mobile devices to the extent possible to reduce the risk of theft and unauthorized access.
- Secure computers and mobile devices with passwords and/or two-factor authentication for highly sensitive information.
- Use secure methods to transfer confidential information.
- Not intentionally damage, alter, misuse any library owned or maintained computing systems, equipment, or networks.

Library Staff

Library staff are ultimately responsible for ensuring that this Cybersecurity Policy and individual responsibilities are clearly communicated to staff and are adequately followed. Specific responsibilities of library managers include:

- Ensuring all staff understand the danger of malicious software, how it is generally spread, and the technical controls used to protect against it.
- Informing the Library Director of the change in status of staff, volunteers, or contract workers who use the library computer resources. This could include a position change (providing greater or more restricted access privileges) or termination of library employment.

GENERAL POLICIES

- The Library Director, Technology Manager, and Meraki are responsible for maintaining the security of the computers. All authorized users of the system are responsible for following all policies and procedures in this policy.

- Server security shall be exclusively controlled by the Library Director, the Technology Manager, and Meraki. Access to server security mechanisms by all other users without prior authorization shall be considered unauthorized access.
- All users must be authenticated to the network before accessing network resources.
- Use of network hardware or software such as traffic monitors/recorders and routers shall be restricted to network management or a designated administrator.
- Security training shall be integrated into existing library training programs such as orientation programs for new employees or volunteers, in the use of computers, software and network information resources.
- Incident logs and subsequent security reports will be generated and reviewed on a regular basis.

ENFORCEMENT

When users fail to comply with this policy, confidential information that is stored, processed, or transmitted on the Lone Cone Library network may be exposed to the unacceptable risk of loss of confidentiality, integrity, or availability. Violations of security guidelines and procedures established to support this policy will be promptly investigated and could result in disciplinary action up to and including termination of employment or termination of rights to use the computer resources.

BREACH OF SECURITY

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

Last date approved: 11/16/2026
Approved by: Lone Cone Library Board of Trustees on 11/17/2025