Geauga County Public Library
Operating Policy Manual

SECTION:	INFORMATION SECURITY
NUMBER:	510
EFFECTIVE DATE:	JUNE 18, 2024

Information security is defined as the administrative, technical, or physical safeguards the Geauga County Public Library "GCPL" uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle confidential customer or staff information "confidential information" and/or financial information.

GCPL will take every reasonable precaution to ensure that any confidential or financial information that is kept by the library for any purpose is safeguarded from unauthorized access. The library has a responsibility to ensure that the accessing, handling, sharing, and disposing of confidential information complies with Confidentiality of Customer Records and Protection of Personal Information Policy of the Geauga County Public Library, the Confidential Information Rules for the CLEVNET System, and Ohio Revised Code Chapter 1347. Within the credit cardholder data environment, the library will also comply with the latest revision of the Payment Card Industry Data Security Standards (PCIS DSS).

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, administrators, and contractors using the library's computer resources.

ROLES AND RESPONSIBILITIES

Under the guidance of the library Director, the IT Manager 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. The IT Manager, along with CLEVNET IT 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.

SECTION:	INFORMATION SECURITY
NUMBER:	510
EFFECTIVE DATE:	JUNE 18, 2024

Authorized Users

Authorized users may be staff members, CLEVNET staff, 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:

- Notify their manager, IT Manager, and IT staff 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 the computer by locking the door or using security cables or devices.
- 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 by requiring passwords (except for public computers with no confidential information). Passwords are integral to security. To minimize the risk of a password being compromised or unauthorized access, follow provided guidelines.
- Use secure methods to transfer confidential information. CLEVNET-provided email systems are enabled with encryption capabilities on demand.
- Not intentionally damage, alter, misuse any library owned or maintained computing systems, equipment, or networks.

Fiscal Office Staff

Fiscal Office staff are ultimately responsible for safeguarding all financial information for the library, its employees, as well as library vendors. Fiscal Office staff will be trained to identify fraudulent attacks such as spear phishing and redirect or business compromise schemes. The Fiscal Officer is responsible for implementing procedures that mitigate the possibility of fraudulent payments.

Library Managers

Library Managers, with guidance or direction from the IT Manager, are ultimately responsible for ensuring that this information security policy and individual responsibilities are clearly communicated to staff and are adequately followed. Specific responsibilities of library managers include:

- Ensuring staff understand the danger of malicious software, how it is generally spread, and the technical controls used to protect against it.
- Informing the IT Manager and IT staff of the change in status of staff, volunteers, or contact 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 IT Manager, IT department staff, and CLEVNET IT are responsible for maintaining the security of the computer. 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 IT Manager, Server and Software Specialist, and CLEVNET IT. Access to server security mechanisms by all other users without prior authorization shall be considered unauthorized access.
- Each authorized user will be assigned a unique user ID and initial password according to the 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.
- 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 Geauga County Public 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 used the computer resources.

SECTION:	INFORMATION SECURITY
NUMBER:	510
EFFECTIVE DATE:	JUNE 18, 2024

BREACH OF SECURITY

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

Approved June 18, 2024