INFORMATION SECURITY

Information security is defined as the administrative, technical, or physical safeguards that Solvay Public Library (Library) uses to access, collect, process, protect, store, use, transmit, dispose of, or otherwise handle confidential customer or staff information (confidential information).

POLICY STATEMENT

It is the policy of the Solvay Public Library (Library) to take every reasonable precaution to ensure that any confidential 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 is done so in a safe and secure manner.

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 and volunteers when using the Library's resources.

ROLES AND RESPONSIBILITIES

Under the guidance of the Board of Trustees, the Library Manager will be designated to oversee the Library's information security program. This will address potential risks to the security, confidentiality and integrity of confidential information that could result in a compromise. The following guidelines will be considered on computing systems, equipment, or networks 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 systems 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 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 are staff members. 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.
- Secure all staff computers by using a screen saver or built-in lock feature when the user physically walks away from the workspace.
- Secure computers and mobile devices with passwords and/or two-factor authentication for highly sensitive information.
- Not intentionally damage, alter, misuse any library owned or maintained computing systems, equipment, or networks.

Library Manager

Library Managers is ultimately responsible for ensuring that this Information Security policy and individual responsibilities are clearly communicated to staff and are adequately followed. Specific responsibilities of the Library Manager includes ensuring staff understand the danger of malicious software, how it is generally spread, and the technical controls used to protect against it.

BREACH OF SECURITY

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