POLICY

Policy Name	Access and Security Control		
Section & Number	General – G12	**Effective Date**	2025-10-16
Motion Number	2025-96	**Last Review**	2025-10-16
Author	Manager, ICT	**Next Review**	2026
Policy Maintenance	Reviewed by Management		

Policy Statement

The St. Catharines Public Library (SCPL) Board is committed to maintaining a secure and trustworthy digital environment for all of its stakeholders. This policy establishes access and security controls that grant access to resources by the public and staff, while securing the availability, integrity and confidentiality of systems, information and resources. This is accomplished by restricting rights only to individuals or entities that have successfully completed the necessary identification, authentication and authorization procedures.

Scope

This policy applies to all library customers, employees, Board members, and external organizations that may need direct or indirect access to the Library's IT systems, networks or information.
This policy applies to all SCPL provided or supported systems, infrastructure, data and services, unless noted otherwise, including:

- **Locations:** all SCPL locations including central, branches and other mobile locations.

- **Technology:** IT systems, or applications that store, process or transmit information. All network and computer hardware, virtualized environment, storage, software and applications, library-provided mobile devices, and telecommunication systems.

- **Data:** all data including transaction streams, data files, repositories, databases, tables, inputs and outputs used by a system.

- **Security Credentials:** all user accounts, all tokens, all security credentials including all user IDs, functional IDs, machine IDs, admin, root, and super user type accounts.

Definitions

Access Control: Is the process that limits and controls access to resources of a computer system.

Library Board: In this policy refers to the members of the SCPL Board.

Employees: In this policy refers to staff, volunteers, co-op or school internships, etc.

External Organizations: Including consultants, vendors and contractors that require access to systems or networks to complete library business or third-party agencies that may have agreements with the library to provide services and systems.

Library Customers: Library customers who access library services with or without a library card.

Users: In this policy is defined as any user whether Library Customer, staff, volunteers, Library Board members or external organizations that uses SCPL systems to access service or perform any business activity.

Regulations

Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, S.O. 2024, c. 24 - Bill 194

Operational Guidelines

Users

All users are provided with access privileges to library technology resources (including web, networks, applications, and devices) based on the following principles:

- **Open Access:** granting open, unrestricted access to IT resources for users to consume digital services and to support intellectual freedom and discovery.

- **Secure Availability:** balancing open access with availability, and security of technology resources to ensure that digital services are protected against disruption, privacy breaches, and are accessible to all users in a secure manner.

All users are governed by the Internet Use Policy and Code of Conduct while accessing SCPL technology resources and services.

Library Board and Employees
While carrying out library business, the Library Board, employees including volunteers, and external organizations are provided with access privileges to systems and technology (including web, networks, systems, applications and devices) based on the following principles:

- **Need to know:** They will be granted access to systems that are necessary to fulfill their library roles and responsibilities.

- **Least privilege:** They will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

User Education and Transparency
Educating employees and library customers on effective use of systems and ways to protect information and systems will be a priority.

Any questions or concerns from library customers or staff regarding access and security control will be investigated and addressed by ICT staff.