Adoption Date:	March 2022
Revision Date:	
Reference #:	BRD - 33
Category:	Innovation & Technology

Cyber Security

1. PURPOSE

The Brampton Public Library Board is committed to managing cyber security risks effectively, efficiently and in compliance with applicable regulations wherever it conducts business.

This policy is the foundation for all data, information and cyber security activities. It focuses not only on the technology, handling , and transmission of information but also on administrative and operational practices for the protection of all information, data, files, and processing resources.

2. POLICY STATEMENT

It is the intent of this Policy to facilitate the exchange of information while balancing the need for protecting services, balancing risk with available resources.

3. SCOPE

This Policy applies to all employees, board members,vendors, contractors, and consultants, who create, distribute, access, or manage information by means of The Brampton Public Library Board's information technology systems including personal or corporate computers,networks, and communication services by which they are connected.

It equally applies to Library users and Service providers who by nature of their relationship to Brampton Library, are entrusted with confidential or sensitive information.

This policy does not apply to information owned by external parties. These groups are responsible for governing the collection and use of their own information. All Brampton Public Library Board information, including electronic/digital and hardcopy, and technology assets are subject to these policies and standards, regardless of their use or physical location. Every individual is required to read and confirm to comply with the requirements associated within their role. Additional roles and responsibilities will be specified within the policy, as required. This policy does not take the place of or supersede any current legislation.

4. REQUIREMENTS

If any of the following requirements within this policy cannot be met, then that security exemption must be documented and recorded. Exemptions must be approved by the CEO of the Brampton Library.

4.1. Information Classification

Information Classification relates to the protection of information to reduce risk from

unauthorized access regardless of where it resides or how it is stored.

The Brampton Library will classify all stored information that is sensitive or confidential.

The classification for this information will adopt definitions of Information Owner, Custodians and Users . This method will be used to allow for clarification of risk, data loss prevention and retention practices within the organization.

4.2. Security Management

The security of corporate devices, information, applications, systems, and networks is fundamental to the continued success of Brampton Public Library Board.

Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information.

Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of Brampton Public Library Board's information, applications, systems, and networks for authorized Users.

5. Policy Objectives

5.1.1. Leadership and Governance

- A cyber security operational plan will be developed and regularly reviewed by the CEO and Director of Innovation and Technology that will balance managing risk with effective resourcing to achieve improvements in Brampton Public Library Board's approach to cyber security.
- Reports for Cyber Security Awareness Training, Information Risk Management, Data Resiliency, Technical Operational Management, Compliance and Insurance will annually be provided to the Brampton Public Library Board.

5.1.2. Cyber Security Awareness Training

The Brampton Library Senior Management and operational staff will develop annual communication and for for the following topics:

- Acceptance Use Policies
- Password Standards
- Confidentiality
- Privacy
- Ownership
- Security

5.1.3. Information Risk Management

The Brampton Library Board will receive information and be made aware of potential risks in relation to Cyber security and the goal to ensure adequate resources are in place for the protection of the Brampton Library.

5.1.4. Data Recovery / Service Resilience

Business continuity or disaster recovery plans will be developed and aligned at two levels within the organization for each operating unit or office:

a) The application owner - normally the individual who is regularly the business process lead and is the person having authorized the deployment of the application, is responsible for developing a continuity plan for business applications.

b) The Director of Innovation and Technology is responsible for developing a continuity plan for the overall IT environment, including data backup and recovery.

c) The Director of Innovation and Technology will complete annual testing related to restoration of data backups.

5.1.5. Technical Operations Management

The Director of Innovation and Technology is responsible for all data, applications, and networks, new software and IT equipment and will establish Operational Procedures for preventing and mitigating the risks associated with Cyber Security around the following areas of focus:

5.1.5.1. Change Management

Applicable for all operational changes and additions of new solutions for all solutions hosted and maintained by the Brampton Public Library Board.

5.1.5.2. Viruses / Malware

To defend the company from computer viruses and malware, all computers and devices connecting to Brampton Libraries infrastructure must be approved devices and have the standard, authorized antivirus and malware protection software installed.

5.1.5.3. Access

5.1.5.3.1. Devices

- Unmanaged Library devices will require a secure connection managed by the Library to gain access to hosted services.
- Managed devices are managed by Brampton Library and will establish a secure connection to the hosted service including device level policies that will disable the device as required to prevent access.

5.1.5.3.2. Users

- Users using managed devices to gain access to the hosted services remotely will be required perform multi factor authentication to gain access
- Users using unmanaged devices locally or remotely will be required to complete a form of multi factor authentication to gain access.

5.1.5.4. Incident Management

The Brampton Public Library will provide a standardized Incident Management practice for users to report lost or stolen devices, security incidents, loss of available service or request formal change not otherwise captured in the scope of a project.

5.1.5.5. Bring-Your-Own-Device (BYOD)

Brampton Library Staff, Board Members, Contractors or Vendors that bring their own device will be subject to and accepting the conditions of Sections 3, 5 and 6. Staff or Contractors requiring access to the internet only will be classified as Library Customers and subject to the acceptable Internet Use Policy.

Library Customers that bring their own devices must accept the Internet Usage Policy at time of use of every session. The use of this service has no access to the hosted on site services of the Brampton Library.

6. Compliance and Insurance

The Brampton Library Board will maintain Cyber liability Insurance coverage, including ransomware coverage consistent with the City of Brampton.

6.1.1. Compliance

Brampton Library will regularly assess developments within the organization and in the environment, and ensure operational procedures are in place for:

- Continuous Cyber security improvements that will include internal and external audits related to compliance as determined in the annual cyber security plan.
- Management of third party's remote access to the Brampton Public Library Board hosted environment.
- Other policies as required to ensure minimum standards of care are taken by the organization to protect against cyber threats.

6.1.2 Violation

Authorized users of IT resources or access to Brampton Public Library assets or information must comply with this policy. Non-compliance with this policy may result in disciplinary action up to and including termination of employment, privileges and/or

contract relationship. Investigations of non-compliance will be undertaken with due consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations. Prior to using any infrastructure, IT assets and/or information, authorized users should request a clarification through their supervisor if they have any concerns regarding compliance with this policy. A privacy breach may be reported to the appropriate regulatory body, such as the Information and Privacy Commissioner, where applicable. Security breaches or incidents must be reported to the CEO.

7. REFERENCES AND RELATED DOCUMENTS

Government of Canada - Canadian Centre for Cyber Security