8.4 DATA MANAGEMENT POLICY

Purpose

As a provider of services, BACI is required by statutory and contractual obligations to establish, maintain and dispose of records. The purpose of this Data Management Policy is to ensure that BACI manages its data responsibly, and in compliance with the Personal Information Protection Act (PIPA), Freedom of Information and Protection of Privacy Act (FIPPA), Income Tax Act, Employment Standards Act, Charitable Fundraising Act, Canada's Anti-Spam Legislation (CASL), WorkSafeBC, CLBC and MCFD guidelines, and in alignment with industry best practices. This policy applies to all physical and digital data owned, managed, or stored by BACI.

Scope

This policy covers:

- **Physical Data:** Including, but not limited to, paper records, printed documents, notebooks, files, books, letters, photographs, audio or video recordings, laptops, physical hard drives and any other tangible forms of information.
- **Digital Data:** Including, but not limited to, data stored on cloud platforms, shared drives, local servers, email systems, databases, and any other electronic storage media.

Responsibilities

- **IT Department:** Responsible for implementing and enforcing this policy, ensuring that all digital data is stored, archived and deleted in accordance with this policy.
- **Department Heads:** Responsible for ensuring that their departments comply with the data retention and destruction procedures.
- **All Employees:** Responsible for adhering to this policy and for understanding the retention periods and secure disposal methods for data relevant to their role.

Data Classification and Access

Data must be classified according to its sensitivity, confidentiality and value to BACI. The following classifications will be used:

- **Public:** Available to all employees and, where applicable, to the public.
- **Internal**: Data intended for internal use within BACI. Available only to employees and approved interested parties who require it for their work.
- **Confidential:** Data that is sensitive and requires limited access.
- **Highly Confidential:** Data that is critical to the organization and requires strict access controls. Access must be limited to authorized personnel with appropriate clearance. Multi-factor authentication should be used for accessing highly confidential digital data.

Data Storage
All BACI data must be stored in approved locations:

- **Physical Data:** All physical data must be stored securely in locked filing cabinets, locked storage rooms, or other secured areas. Access should be limited to authorized personnel only.
- **Digital Data:** Digital data should be stored on secure servers, cloud storage services, or other secure digital platforms approved by the IT department. Regular backups must be performed to prevent data loss.

Data Retention
Retention periods are determined by legal requirements, funder requirements, accreditation, operational needs, and best practices.

BACI will maintain records for

- Persons served
- Employees
- Volunteers
- Contractors
- Members
- Donors

BACI will also maintain the following records:

- Financial (payroll, accounts, etc.)
- Administrative (attendance, vehicle, etc.)
- Legal (contracts, minutes, etc.)

The following general retention periods apply to BACI data:

- **Financial Records:** 7 years
- **Donor Records:** 7 years
- **Employee Records:** 7 years after termination
- **Individuals Served Records**: 7 years
- **Life Sharing Providers**: 7 years
- **Program Records**: 5 years after the program ends
- **Contracts**: 6 years after expiration
- **Emails**: 5 years
- **Meeting Minutes and Agendas**: Permanently
- **Legal Documents**: Permanently

Specific retention periods for other types of data should be identified in departmental procedures or as required by law.

Data Disposal
When data reaches the end of its retention period or is no longer needed, it must be disposed of securely:

- **Physical Data:** Paper documents must be confidentially shredded or otherwise destroyed so that they cannot be re-constructed or read.
- **Digital Data:** Digital data must be deleted securely, ensuring that it cannot be recovered. This includes using secure deletion tools for electronic files and ensuring that backups are also purged.

Review and Audit

This policy will be reviewed and updated annually or as needed to comply with changes in laws, regulations, or organizational needs.

Linking Policies

1.8 Code of Ethics
8.1 BACI Privacy Policy for Individuals
8.2 Privacy Policy – Plain Language
8.3 BACI Privacy Policy for Employees
8.4 Records Management Policy
8.7 Video Surveillance Policy