## 

### ***Disclaimer***

*This draft foundational document was prepared by a certified cybersecurity/GRC professional and is provided for general information only.* ***It is not legal advice.*** *Obtain independent legal review before adopting or relying on this policy.*

## 

### ***Data Governance & Privacy***

* **Inventory sensitive data**: Identify and list all places sensitive data is collected, stored, and processed (local drives, cloud storage, Google Workspace, payroll tools).
* **Categorize data sensitivity**: Label clearly (e.g., Public, Internal, Confidential, Highly Sensitive).
* **Review privacy obligations**: Ensure collection/use aligns with BC’s PIPA requirements (explicit consent for sensitive data).

**Why?**

Essential for compliance; prevents accidental mishandling or disclosure.

### ***User Access & Account Management***

* **Enable Multi-Factor Authentication (MFA)**: Start immediately for paid staff and volunteers with access to private information or administrative access on critical accounts and services.
* **Review and remove unused accounts regularly** (monthly/quarterly).
* **Implement basic password policy**: Recommend using secure passphrases or password managers.

**Why?**

Immediate, significant boost to security with minimal effort.

### ***3. Website & Application Security***

* **Regular security updates**: Schedule monthly website/CMS updates.
* **Basic vulnerability scanning**: Conduct quarterly scans using free/open-source tools (e.g., OWASP ZAP) and remediate issues.
* **SSL/TLS certificates**: Ensure website uses HTTPS for secure browsing.

**Why?**

Avoid common exploits and protect visitor data.

### ***4. Data Storage & Cross-border Transfers***

* **Clarify cloud service storage**: Verify and document data storage locations (especially if outside Canada—like California).
* **Communicate clearly in privacy policy**: Inform clients/donors about cross-border data storage explicitly.
* **Limit highly sensitive cross-border transfers**: Consider using Canada-based providers for sensitive data (e.g., health info, government-issued IDs).

**Why?**

Mitigate compliance risks around international data transfers.

### ***5. Backup & Disaster Recovery***

* **Establish regular backups** (weekly minimum): Clearly document backup procedures for website and cloud data.
* **Test data recovery process**: Conduct a bi-annual restore test.
* **Secure backup data**: Store backups securely and encrypted, preferably off-site or cloud.

**Why?**

Crucial for business continuity; inexpensive and easy to implement.

### ***6. Incident Response & Basic Preparedness***

* **Simple incident response plan**: Define basic steps (e.g., who to call if breached, what data to check first).
* **Prepare breach notification templates**: For quick compliance with BC PIPA mandatory breach-reporting.
* **Assign an internal cybersecurity contact**: Even if part-time, someone to coordinate responses and maintain records.

**Why?**

Helps quickly contain and reduce damage in incidents.

### ***7. Awareness & Training***

* **Brief annual cybersecurity awareness training**: Free resources available online (Govt. of Canada, BC Gov., CIRA).
* **Regular reminders**: Monthly email on phishing and safe online practices.

**Why?**

Human error is the most common vulnerability; inexpensive to address.

### ***8. Policy Review & Documentation***

* **Update old privacy & terms policies**: Revise outdated documents, clearly stating current data handling practices.
* **Simple, practical policy templates**: Acceptable Use, Privacy Policy, and Data Retention basics.

**Why?**

Demonstrates clear organizational responsibility and accountability.

***9. Monitoring & Basic Logging***

* **Activate logging** on web servers or critical applications.
* **Simple monthly log reviews**: Check for unusual patterns (failed login attempts, odd access times).

**Why?**

Early detection of suspicious activity is highly beneficial and cost-effective.

### ***10. Future Considerations (Growth)***

* **Explore cyber insurance options**: Low-cost, basic coverage options may be appropriate as the charity grows.
* **Plan for PCI-DSS compliance**: Document current payment gateway compliance and anticipate any future requirements.

**Why?**

Forward-looking measures that protect the organization’s longevity.

**Implementation Notes:**

* Tasks marked as immediate actions (MFA, inventory, backups) provide the highest ROI for minimal effort.
* Delegate clear responsibilities internally, or engage knowledgeable volunteers.