## 

### ***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.*

## 

### ***1. Purpose & Scope***

## This standard outlines how personal data must be handled, stored, and retained by Oak Bay Volunteer Services across all systems, services, volunteers, and third-party tools. It applies to all data collected via our website, app, cloud systems, and offline processes.

## It aims to ensure compliance with:

## BC Personal Information Protection Act (PIPA)

## Canada Revenue Agency (CRA) record-keeping rules

## Employment Standards Act (ESA)

## PCI-DSS (where applicable)

## OWASP security practices

## Any applicable PIPEDA provisions

## 

### 

### 

### 

### ***2. Roles & Responsibilities***

| **Role** | **Responsibility** |
| --- | --- |
| Data Steward | Oversees data lifecycle, ensures appropriate classification and handling. |
| System Owner | Maintains the technical environment where data resides. |
| Volunteers & Staff | Must follow handling, storage, and destruction guidelines outlined here. |
| Executive Director | Final decision-maker on data-related exceptions or escalations. **[TODO: Confirm title]** |

## 

### ***3. Information Classification***

## All data must be classified into one of four tiers:

| **Classification** | **Description** |
| --- | --- |
| Public | Safe for unrestricted disclosure (e.g., published program info). |
| Internal | For internal use only (e.g., non-sensitive planning docs). |
| Confidential | Could cause harm if disclosed (e.g., donor lists, employee records). |
| Highly Sensitive | Could cause significant harm (e.g., ID scans, health data). |

## 

### ***4. Storage & Protection***

## **Minimum security controls** for storing or handling personal information:

## Encryption at rest and in transit for Confidential and Highly Sensitive data.

## Two-factor authentication (2FA) on systems storing such data.

## Tokenization for payment info via third-party processors.

## Access controls (role-based access, least privilege).

## Log scrubbing of IPs and identifiers beyond troubleshooting period.

## **Examples:**

## Google Drive access restricted by role, with 2FA enabled.

## Email containing ID scans must be encrypted or deleted after download.

## No personal data stored on volunteer devices unless encrypted.

## 

### ***5. Retention Schedule***

| **Data Type** | **Retention Period** | **Legal Basis/Trigger** | **Storage Location** |
| --- | --- | --- | --- |
| Donation & Tax Receipts | 7 years | CRA | [TODO: specify] |
| HR & Volunteer Records | Up to 7 years after role ends | ESA, CRA | [TODO: specify] |
| ID Documents | Delete after verification/use ends | PIPA ss 11, 35 | [TODO: specify] |
| Client Health/Accommodation Info | While services are active | PIPA ss 11, 35 | [TODO: specify] |
| Staff-Client Interaction Notes | Until case/program ends + 1 year | Operational practice | [TODO: specify] |
| Technical Logs | 30–90 days | Troubleshooting & security monitoring | [TODO: specify] |

## When retention ends, data must be securely destroyed or anonymized.

## 

### ***6. Secure Destruction***

## **Examples of secure deletion:**

| **Method** | **Example Command** |
| --- | --- |
| Local file deletion | shred -u sensitive\_file.txt |
| Cloud storage | aws s3 rm s3://[bucket]/folder/ --recursive |
| Google Drive | Manual delete + empty trash + audit access logs |

## **Verification steps:**

## Confirm file deletion in UI or command line.

## Log date, method, and user performing deletion.

## For sensitive data, destruction should be verified by a second party or supervisor.

## 

### ***7. Cross-Border Processing [If relevant]***

## Some data may be processed or stored in the U.S. or other jurisdictions (e.g., cloud email, form submissions, CRM).

## We notify users in our Privacy Policy and obtain informed consent (PIPA s 30.1).

## **[TODO: List specific tools/systems hosted outside Canada]**

## 

### ***8. Link to Incident Response***

## For breach notification and mitigation steps, refer to our: **[Incident Response Playbook – link or location TBD]**

## Staff and volunteers must report any suspected data breach immediately to: **[TODO: insert Privacy Officer or Data Steward contact]**

## 

### ***9. Version Control & Review***

| **Version** | **Date** | **Notes** |
| --- | --- | --- |
| 0.9 | 24 May 2025 | First draft — for internal discussion. |

## This document should be reviewed:

## At least annually

## Or after any significant system or legal change

## 

### **10. Final Notes**

## Training on this standard is recommended for all staff and volunteers handling personal data.

## Exceptions to this standard must be documented and approved by the Executive Director or their delegate.

## Questions or clarifications should be directed to the Data Steward or Privacy Officer.

## 