Customer Data Privacy Policy (PIPEDA Compliance)

1.0 Policy Objective & Scope

The objective of this policy is to ensure that all customer personal information collected, used, or disclosed by the company is handled in strict compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA). This policy establishes clear guidelines for obtaining consent, limiting collection, ensuring accuracy, safeguarding data, and providing individuals with access to their information.

This policy applies to all employees, contractors, and third-party service providers who have access to customer personal information in any form, including electronic records, paper files, and verbal communications. It covers all departments, including sales, customer support, manufacturing, shipping, and IT.

2.0 Roles & Responsibilities

- Privacy Officer (Designated by CEO): Oversees PIPEDA compliance, handles privacy complaints, and approves data sharing agreements.
- **IT Administrator:** Implements technical safeguards (encryption, access controls), manages data retention schedules, and assists with breach investigations.
- **Department Heads:** Ensure their teams follow the policy, approve data collection requests, and report any suspected breaches immediately.
- **All Employees:** Must complete annual privacy training, obtain proper consent before collecting data, and report any unauthorized access or loss of data.

3.0 Core Rules & Guidelines

- Customer personal information may only be collected for purposes that a reasonable person would consider appropriate in the circumstances, and only with informed consent.
- Consent must be obtained at the time of collection or before use/disclosure, and must be explicit for sensitive information (e.g., financial, health).
- Personal information must be retained only as long as necessary to fulfill the identified purposes, and then securely destroyed or anonymized.
- All electronic customer data must be encrypted at rest (AES-256) and in transit (TLS 1.2+). Paper records must be stored in locked cabinets accessible only to authorized personnel.
- Access to customer data is granted on a need-to-know basis only. Any access outside of job duties is a violation of policy.
- Data breaches involving personal information must be reported to the Privacy Officer within 24 hours of discovery, and to the Office of the Privacy Commissioner of Canada if there is a real risk of significant harm.

4.0 Step-by-Step Procedure / Workflow

1. Identify the specific personal information required and document the purpose for collection on the Data Collection Request Form in SwitchDesk.

2. Obtain informed consent from the customer using the approved consent script or form, ensuring they understand how their data will be used and stored.

3. Record the consent in the customer's digital profile in the CRM, including the date, method of consent, and scope of consent.

4. Store the collected data in the designated secure folder on the company server or encrypted cloud storage, with access restricted to authorized personnel only.

5. If the data is no longer required for the original purpose (e.g., after warranty period expires), initiate the data destruction request in SwitchDesk.

6. The IT Administrator verifies the destruction request and securely deletes electronic files using approved wiping software or physically shreds paper documents.

7. Log the destruction in the Data Disposal Log, including the date, method, and witness signature (if applicable).

8. If a customer requests access to their personal information, direct them to the Privacy Officer who will verify identity and provide the information within 30 days.

9. If a data breach is suspected, immediately isolate the affected system and notify the Privacy Officer and IT Administrator via the emergency contact list.

10. The Privacy Officer leads the breach investigation, documents findings, and determines if notification to the Privacy Commissioner and affected individuals is required.

11. Implement corrective measures (e.g., patch vulnerabilities, retrain staff) and update the policy as needed to prevent recurrence.

12. Conduct an annual review of all data collection practices and update consent forms and privacy notices as required by changes in PIPEDA or business operations.

5.0 Documentation & Compliance

1. All consent records, data access logs, and destruction logs must be retained for at least three years after the data is no longer in use, as required by PIPEDA.

2. Store signed consent forms and data access requests in the customer's secure digital file in SwitchDesk, with access limited to the Privacy Officer and authorized department heads.

3. Maintain a central Data Breach Response Log that documents every breach incident, investigation steps, and corrective actions taken.

4. The Privacy Officer must conduct a semi-annual audit of data handling practices, reviewing a random sample of customer files for compliance with this policy.

5. All employees must complete an annual PIPEDA compliance training module and sign an acknowledgment of this policy, with records kept in the HR file.

6. Any third-party service providers who handle customer data must sign a data processing agreement that mirrors this policy and submit to periodic audits.

Regulatory Disclaimer: This document is a generic administrative template provided for educational purposes. The end-user assumes all liability for reviewing, adapting, and validating all protocols against organizational policies.