PTI CABLES INC.

Privacy Governance Policy and Practices

Internal policy governing the protection of personal information

Document type	Internal policy (Law 25, s. 3.2)
Effective date	August 20, 2026
Version	1.0
Owner / approver	Privacy Officer / Management
Review cycle	Annual, or on significant change

This policy sets out the internal roles, rules and controls Cables PTI Cables Inc. ("PTI Cables", "PTI") follows to protect personal information and to comply with Quebec's Law 25. It is proportionate to the sensitivity and volume of information PTI holds, and it supports the commitments made in PTI's external Privacy Policy. A plain language summary of these practices is made available to individuals as required by law.

1. Scope

This policy applies to all PTI employees, officers, contractors and anyone acting on PTI's behalf, and to all personal information PTI collects, uses, communicates, retains or destroys, whether about employees, applicants, customers, suppliers or website users, in any format.

2. Governance roles and responsibilities

2.1 Person in charge (Privacy Officer)

By law, the person with the highest authority at PTI is responsible for protecting personal information. That responsibility has been delegated in writing to the Privacy Officer named below, who oversees the privacy program, approves privacy practices, handles rights requests and complaints, leads incident response, and is the published point of contact.

> **Designated Privacy Officer:** Elie Bengio, Chief Information Officer, ebengio@pticables.com, 514-531-8705
> **Delegated by:** Daniel Lieberman, Co President, with effect from November 1, 2025
> **Written instrument:** Designation of the Person in Charge of the Protection of Personal Information, Evidence Binder Tab 01

2.2 Managers and staff

Managers ensure their teams follow this policy. All staff must collect and use personal information only for legitimate, identified purposes, limit access to those who need it, protect information in their care, and report any suspected confidentiality incident to the Privacy Officer without delay.

3. Core privacy practices

3.1 Limiting collection (minimization)

We collect only the personal information necessary for a specific, identified purpose. We do not collect sensitive information (such as SINs or health information) unless it is genuinely necessary or legally required.

3.2 Purpose and consent

We identify the purpose before or at the time of collection and obtain valid consent where required: free, informed and specific, and express for sensitive information. Consent is documented. Requests for consent are presented separately and in clear language. We do not use pre-checked boxes.

3.3 Privacy by default

For any product, service or system that collects personal information, the strictest privacy settings apply by default without any action required by the individual.

3.4 Use, sharing and third parties

Personal information is used only for the purposes for which it was collected. Before sharing information with a service provider (for example, benefits providers), we ensure a written agreement is in place requiring the provider to protect the information, use it only for the mandated purpose, and return or destroy it when the work is done.

3.5 Transfers outside Quebec

Before communicating personal information outside Quebec, the Privacy Officer conducts (or reviews) a privacy impact assessment considering the sensitivity of the information, the purpose, the safeguards in place, and the legal framework of the destination. The transfer proceeds only if the information will receive adequate protection, under a written agreement.

3.6 Retention and destruction

Personal information is kept only as long as necessary for the identified purposes or as required by law, then securely destroyed or anonymized in accordance with PTI's Data Retention and

Destruction Schedule.

3.7 Security safeguards

We apply reasonable physical, organizational and technological safeguards proportionate to sensitivity, including access controls on a need-to-know basis, secure storage, protection of devices and accounts, and secure disposal. Access to sensitive information is further restricted and, where feasible, logged.

4. Privacy impact assessments (PIAs)

A PIA is completed, using PTI's PIA template, before PTI acquires, develops or overhauls an information system or electronic service delivery project involving personal information, and before any transfer of personal information outside Quebec. The Privacy Officer maintains completed PIAs on file.

5. Individual rights

Individuals may exercise their rights of access, rectification, withdrawal of consent, de-indexing and portability, as described in PTI's Rights Request Procedure. Requests are logged and answered within 30 days. The Privacy Officer is responsible for handling them.

6. Confidentiality incidents

All suspected or actual confidentiality incidents are managed under PTI's Confidentiality Incident Response Procedure. PTI maintains a register of confidentiality incidents and keeps each entry for at least five years. Where an incident presents a risk of serious injury, PTI notifies the CAI and affected individuals promptly.

7. Training and awareness

The Privacy Officer provides periodic awareness briefings to staff who handle personal information, covering their obligations, how to recognize and report an incident, and how to handle rights requests. A simple record of who was trained and when is maintained.

8. Records the Privacy Officer maintains

- This policy and the external Privacy Policy, with version history;
- The written designation and delegation of the Privacy Officer;
- Consent records;

- The register of confidentiality incidents (kept 5 years per entry);
- The log of individual rights requests;
- Completed PIAs and third-party and transfer assessments;
- The data retention and destruction schedule and destruction records;
- Training records.

9. Review

This policy is reviewed at least annually and whenever there is a significant change to PTI's activities, systems or the law. Changes are approved by the Privacy Officer and, where material, by Management.

Approved by: ________________________________

Name / title: ________________________________ Date: ___________________