Privacy Management Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	P1.1, P2.1, P3.1, P3.2, P4.1, P4.2, P4.3, P5.1, P5.2, P6.1, P6.2, P6.3, P6.4, P6.5, P6.6, P6.7, P7.1, P8.1

Table 2: Document history

Date	Comment
Apr 21 2026	Completed policy for SOC 2 Privacy TSC
Sep 3 2026	Added Alberta PIPA, PII matrix, and Privacy by Design

1 Purpose and Scope

a. The purpose of this policy is to establish CredX's commitment to protecting the privacy of personal information collected, processed, stored, and disclosed in the course of its operations.

b. This policy applies to all personal information handled by CredX, including information about customers, employees, contractors, and other individuals, regardless of the format in which it is held.

c. This policy applies to all employees, contractors, vendors, and third parties who collect, access, process, or transmit personal information on behalf of CredX.

2 Background

a. CredX collects and processes personal information as part of delivering its embedded lending, credit decisioning, and payments products. Because CredX handles regulated personal and financial data on behalf of regulated partners, and because its consumer proposition is explicitly built on data control and consent, privacy is a core control domain rather than a compliance formality.

b. **Applicable regime.** CredX, as an Alberta-incorporated organization, is primarily governed by **Alberta's Personal Information Protection Act (PIPA)** rather than PIPEDA for its own operations, since Alberta is a "substantially similar" jurisdiction. **PIPEDA** continues to apply to interprovincial or international handling of personal information, which is realistic given merchants and processors located outside Alberta. In practice CredX must meet both standards, which are substantively similar.

c. **Scope caution.** CredX's Business Requirements Document additionally names GDPR and CCPA. Whether those regimes genuinely apply depends on where CredX's users and merchants are located. Confirming CredX's operating jurisdictions, and scoping this policy accordingly, is a tracked action item. CredX must not claim alignment with frameworks that do not apply to it.

d. **Status.** CredX's privacy program is **in development**. The breach protocol below is defined; standalone data classification, retention, and access control policies are not yet fully issued; and user-facing consent, notice, and self-service access/deletion mechanisms are not yet confirmed as implemented. The CredX website currently carries a "PIPEDA Compliant" trust marker — resolving the gap between that claim and this status is a tracked action item owned by the CEO.

3 Definitions

a. **Personal Information**: Any information about an identifiable individual, including name, email address, phone number, financial data, location data, online identifiers, and any other data that can identify a natural person directly or indirectly.

b. **Data Subject**: An individual whose personal information is collected or processed by CredX.

c. **Processing**: Any operation performed on personal information, including collection, storage, use, disclosure, transfer, and deletion.

d. **Data Controller**: CredX, as the entity that determines the purposes and means of processing personal information. Note that CredX is the controller for personal information on its platform **even though the checkout carries the merchant's brand** — brand attribution does not transfer privacy-law accountability.

e. **RROSH**: "Real risk of significant harm", the trigger for mandatory breach notification under both PIPA and PIPEDA.

f. **De-identified**: Personal information altered such that an individual can no longer reasonably be identified from it, whether directly or by combination with other available data.

4 Policy

4.1 Privacy Notice and Transparency (P1.1)

a. CredX must provide clear and accessible privacy notices to data subjects at or before the point of collection. Privacy notices must describe:

   i. The categories of personal information collected.

   ii. The purposes for which personal information is collected and used.

   iii. The legal basis for processing (where applicable).

   iv. How long personal information is retained.

   v. Whether personal information is shared with third parties, and for what purposes.

   vi. Data subjects' rights regarding their personal information.

   vii. Contact information for privacy inquiries or complaints.

b. Privacy notices must be reviewed and updated whenever there is a material change to CredX's data practices. Data subjects must be notified of material changes in a timely manner.

4.2 Consent and Choice (P2.1)

a. Where consent is the legal basis for processing, CredX must obtain explicit, informed, and freely given consent from data subjects prior to collecting or processing their personal information.

b. Data subjects must be informed of the consequences of withholding consent. Consent must not be a condition of service where processing is not strictly necessary.

c. Data subjects must be provided with meaningful choices regarding the collection, use, retention, disclosure, and disposal of their personal information.

d. Consent must be documented and retained as evidence. Data subjects may withdraw consent at any time; withdrawal must be honoured promptly and without detriment.

4.3 Collection of Personal Information (P3.1, P3.2)

a. CredX must collect only the minimum personal information necessary to fulfill the stated purpose (data minimization principle).

b. Personal information must be collected through lawful and fair means.

c. For categories of personal information requiring explicit consent (e.g., sensitive personal data such as health information, biometric data, or financial account details), CredX must:

   i. Clearly communicate to the data subject why such information is needed.

   ii. Inform the data subject of the consequences of not providing consent.

   iii. Obtain explicit consent before collection.

4.4 Use, Retention, and Disposal (P4.1, P4.2, P4.3)

a. Personal information must only be used for the purposes for which it was collected, as described in the applicable privacy notice, or as otherwise permitted by law.

b. Personal information must not be used for secondary purposes without obtaining fresh consent or establishing another lawful basis for processing.

c. Personal information must be retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by law. Retention periods are defined in CredX's Data Retention Policy.

d. Upon expiry of the retention period, personal information must be securely disposed of using methods that prevent reconstruction or recovery, in

accordance with CredX's Data Classification Policy and Data Retention Policy.

4.5 Data Subject Access and Amendment (P5.1, P5.2)

a. Data subjects have the right to request access to their personal information held by CredX. Upon verified request, CredX must:
   i. Confirm whether personal information is held.
   ii. Provide a copy of the personal information in a readable format within the timeframe required by applicable law (generally 30 days).
   iii. If access is denied (e.g., where it would affect the rights of others), inform the data subject of the denial and the reason.

b. Data subjects have the right to request correction or amendment of inaccurate or incomplete personal information. CredX must:
   i. Correct or append the record promptly upon verified request.
   ii. Notify any third parties to whom the information was disclosed of the correction, where required.
   iii. If a correction request is denied, inform the data subject and provide the reason.

4.6 Disclosure to Third Parties (P6.1–P6.7)

a. Personal information must not be disclosed to third parties without the explicit consent of the data subject, unless disclosure is:
   i. Required by law or court order.
   ii. Necessary for the delivery of services via an authorized sub-processor.
   iii. Otherwise permitted under applicable privacy law.

b. CredX must maintain a record of all authorized disclosures of personal information, including the recipient, purpose, date, and legal basis.

c. CredX must maintain a record of any detected or reported unauthorized disclosures (including data breaches), in accordance with the Security Incident Response Policy.

d. All third parties and vendors who access personal information must provide contractual privacy and security commitments (e.g., via a Data Processing Agreement). Vendor compliance with these commitments must be assessed at least annually for Tier 1 vendors.

e. CredX must obtain commitments from vendors that they will notify CredX immediately upon discovery of actual or suspected unauthorized disclosure

of personal information. Such notifications must be handled in accordance with the Security Incident Response Policy.

f. In the event of a personal data breach, CredX must notify affected data subjects, applicable regulatory authorities, and other required parties in accordance with the Security Incident Response Policy and applicable law.

g. Data subjects may request an accounting of disclosures of their personal information. CredX must provide such an accounting within the timeframe required by applicable law.

4.7 Accuracy (P7.1)

a. CredX must take reasonable steps to ensure that personal information is accurate, complete, up-to-date, and relevant for the purposes for which it is used.

b. Employees who become aware of inaccurate personal information must report it to the relevant data owner for correction.

4.8 Dispute Resolution and Complaints (P8.1)

a. CredX must maintain a process for receiving, addressing, and resolving privacy inquiries, complaints, and disputes from data subjects.

b. A designated Privacy Contact (the ISM or appointed delegate) must be responsible for receiving and responding to privacy complaints.

c. Complaints must be acknowledged within 5 business days and resolved within 30 calendar days, or as required by applicable law. Data subjects must be informed of the outcome.

d. If a complaint cannot be resolved internally, data subjects must be informed of their right to escalate to the applicable regulatory authority.

e. CredX must monitor compliance with this policy and take corrective action where deficiencies are identified.

4.9 PII Classification and Handling Requirements

a. PII includes, but is not limited to: name, email, phone number; government-issued identifiers; device identifiers when linked to an individual; and transaction metadata tied to identifiable users.

b. All data must be classified as **Public, Internal, Confidential, or Restricted** (PII/payment-related). This scheme complements the sensitivity tiers used in the Data Classification Policy.

c. The following handling requirements apply:

Requirement Area	Controls
Collection & Minimization	Collect only the minimum PII required for business operations; avoid storing PII in mobile apps wherever possible; **do not embed PII in QR codes or URLs**
Encryption & Storage	Encrypt PII at rest using AES-256 or stronger; use field-level encryption for high-risk attributes; store encryption keys separately from encrypted data; use unique keys per environment
Access Controls	Enforce role-based access control; restrict PII access to authorized services and personnel only; require MFA for any administrative access to PII; log and audit all PII access events
Transmission	Transmit PII only over TLS 1.2+ secured channels; use tokenization when sharing data with third parties; **prohibit PII in logs, analytics, crash reports, and monitoring tools**
Retention & Deletion	Define retention policies per PII category; automatically purge PII when no longer required; support user-initiated deletion requests; **ensure backups respect retention and deletion policies**
Incident Response for PII	Detect unauthorized access to PII; provide immediate key rotation and token revocation; notify stakeholders and partners per contractual obligations; maintain documented breach response procedures per the Security Incident Response Policy

a. **Data residency.** PII and sensitive customer data must be processed and stored within Canada-based infrastructure. Heroku Private Spaces in the Canadian region are used to meet the data residency expectations of Canadian enterprises and regulated partners. Cross-border data transfers must be explicitly reviewed, documented, and approved.

4.10 Consent Management

a. CredX's consumer proposition is built on user control of personal data. Consent is therefore a **primary control**, not a user-interface feature, and must be implemented and evidenced as such.

b. Consent must be **granular** — recorded per data source and per purpose — and captured through plain-language consent flows.

c. Consent must be **revocable at any time**. Revocation must propagate: data shared under a consent later withdrawn must cease to flow, must cease to be used as a model input under the Artificial Intelligence Governance

Policy, and downstream copies must be addressed under the retention and deletion requirements above.

d. Users must be able to see **where and how their data has been used**, through accessible activity logs.

e. Data collected for one purpose must not be silently repurposed for another. Decisioning data must not be repurposed for personalization, targeting, or merchant analytics without a fresh, documented consent, and vice versa.

f. Consent records must be retained as part of the audit trail CredX maintains to support regulated partners' compliance and incident processes.

g. **Open banking connections** and linked loyalty or purchase-history sources are high-sensitivity data sources collected under consent, and are governed by the same PII handling requirements as credit bureau data.

4.11 De-identification and Merchant Analytics

a. Merchant-facing analytics derived from consumer data must be **de-identified before disclosure**, and must not be presented at a granularity that permits re-identification.

b. Re-identification of de-identified data, or any attempt to do so, is prohibited.

c. Because CredX markets merchant insight as opt-in by default, consent-driven, and de-identified, each of those three properties must be independently evidenced on request. A marketing claim that cannot be evidenced is a due-diligence exposure.

4.12 Credit Bureau Data and Permissible Purpose

a. Credit bureau responses, credit scores, and underwriting outputs are handled **strictly under the licensed lender's permissible purpose**. They must not be resold or repurposed, and all access must be logged.

b. A permissible-purpose failure is a regulatory event for the lending partner, not only for CredX. The consequences of that accountability structure are described in the Security Incident Response Policy.

4.13 Privacy by Design

a. CredX grounds its PII handling in the seven Privacy by Design principles developed by Dr. Ann Cavoukian, former Information & Privacy Commissioner of Ontario.

Principle	How CredX Applies It
1. Proactive not Reactive; Preventative not Remedial	PII minimization, encryption, and QR-design requirements are built in before any data is collected
2. Privacy as the Default	PII is never embedded in QR codes or URLs by default; the most privacy-protective setting applies unless a business need is explicitly documented; merchant insight is opt-in by default
3. Privacy Embedded into Design	Encryption, tokenization, and access control are core architecture requirements in the Security Architecture Narrative, not later additions
4. Full Functionality — Positive-Sum, not Zero-Sum	The QR and wallet design achieves both fraud prevention and user convenience without exposing PII
5. End-to-End Security — Lifecycle Protection	Encryption, storage, retention, and deletion controls cover data from collection through secure destruction
6. Visibility and Transparency	Logging and auditing requirements, plus the annual review and approval process for this program and the underlying security specification
7. Respect for User Privacy	**Known gap.** The technical controls exist, but user-facing consent, notice, and self-service data access/deletion mechanisms are not yet confirmed as implemented. Closing this is a tracked action item.

a. Principle 7 is the one open gap in CredX's Privacy by Design posture. It is material because CredX's consumer-facing promise — that users control their data and can see how it is used — currently runs ahead of the verified control.

5 Roles and Responsibilities

a. The **Information Security Manager (ISM)** serves as the Privacy Contact and is responsible for overseeing compliance with this policy, responding to data subject requests and complaints, and coordinating breach notification.

b. The ISM role at CredX is held jointly by the **Chief Technology Officer (CTO)** and the **Founder & CEO**. The **CTO** acts as the operational Privacy Contact, receiving and responding to data subject requests, privacy inquiries, and complaints, and coordinating breach investigation and notification. The **Founder & CEO** is the executive accountable for the privacy

program, including decisions on regulatory notification and escalation to data protection authorities. The Privacy Contact is published in CredX's privacy notices as the route for privacy inquiries and complaints.

c. All **employees and contractors** are responsible for handling personal information in accordance with this policy and for reporting any suspected privacy incidents or breaches immediately to the ISM.

d. **Managers** are responsible for ensuring their teams understand and follow this policy.

6 Enforcement

a. Violations of this policy may result in disciplinary action up to and including termination of employment or contract. Violations that constitute a breach of applicable law may be referred to the appropriate regulatory authority.