Vendor Management Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.2

Table 2: Document history

Date	Comment
Sep 3 2026	Added critical vendor register and tiering

1 Purpose and Scope

a. This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners.

b. This policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of the organization's technology and sensitive information, or who are within the scope of the organization's information security program.

c. This policy applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of the organization.

2 Background

a. The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

3 References

a. Information Security Policy

b. Security Incident Response Policy

4 Policy

a. IT vendors are prohibited from accessing the organization's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

b. All IT vendors must comply with the security policies defined and derived from the Information Security Policy (reference (a)).

c. All security incidents by IT vendors or partners must be documented in accordance with the organization's Security Incident Response Policy (reference (b)) and immediately forwarded to the Information Security Manager (ISM).

d. The organization must adhere to the terms of all Service Level Agreements (SLAs) entered into with IT vendors. As terms are updated, and as new

ones are entered into, the organization must implement any changes or controls needed to ensure it remains in compliance.

e. **Vendor Risk Tiering:** All IT vendors must be classified into one of the following risk tiers based on their access to organizational systems and data:
   i. **Tier 1 – Critical Vendors**: Vendors with direct access to production systems, sensitive data, or personal information. These vendors present the highest risk and require the most rigorous due diligence.
   ii. **Tier 2 – Significant Vendors**: Vendors with indirect or limited access to organizational systems, or whose service failures would have moderate business impact.
   iii. **Tier 3 – Standard Vendors**: Vendors with no access to organizational systems or sensitive data.

f. **Vendor Due Diligence Requirements by Tier:**
   i. **Tier 1 Vendors** must, before access is granted and annually thereafter:
      1. Provide a current SOC 2 Type II report or equivalent third-party security certification (ISO 27001, PCI DSS, etc.). The report must be reviewed by the ISM or delegate.
      2. Complete a vendor security questionnaire.
      3. Undergo a supply chain risk assessment identifying sub-processors and sub-suppliers.
      4. Sign a Data Processing Agreement (DPA) if processing personal data.
   ii. **Tier 2 Vendors** must complete a vendor security questionnaire before access is granted and annually thereafter.
   iii. **Tier 3 Vendors** require basic contractual security clauses only.

g. Before entering into a contract and gaining access to organizational information systems, all IT vendors must undergo a risk assessment proportional to their tier classification.
   i. Security risks related to IT vendors and partners must be identified during the risk assessment process.
   ii. The risk assessment must identify risks related to information and communication technology, as well as risks related to IT vendor supply chains, including sub-suppliers.

h. **Annual Vendor Review:** All Tier 1 vendors must be reviewed annually. The ISM is responsible for maintaining a vendor register and scheduling reviews. Reviews must confirm continued compliance with security requirements and assess any changes in risk.

i. IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The organization strictly adheres to all applicable legal, regulatory, and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).

j. The organization may audit IT vendors and partners at any time to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.

5 CredX Critical Vendor Register

a. The following vendors and partners are within scope of this policy. Tiering reflects the criticality assessment in the Business Continuity Plan.

Vendor / Partner	Service	Tier	Owner
Ownest Inc.	Credit underwriting and loan-terms decisioning; licensed technology stack behind UnderwriteFlow. **Affiliated company — shared CTO**	Tier 1	Kendall Raessler / Ray Yip
Heroku (Salesforce)	Backend hosting — Private Spaces, Canadian region	Tier 1	Ray Yip
Clover	POS provider — order source and payment tender destination (OAuth v2, auto-refresh)	Tier 1	Ray Yip
Square	POS provider — order source and payment record destination (static admin-pasted token)	Tier 1	Ray Yip
Apple Wallet / APNs	Payment instrument — wallet pass and push updates	Tier 1	Ray Yip
Google Wallet	Payment instrument — wallet pass	Tier 1	Ray Yip
Sign in with Apple / Google	Customer authentication at account creation and login	Tier 1	Ray Yip
Twilio	SMS delivery — login codes and OTP	Tier 2	Ray Yip
SendGrid	Email delivery — OTP and administrative links	Tier 2	Ray Yip
Expo Push	Mobile push delivery — merchant order alerts	Tier 2	Ray Yip
AWS S3	Object storage — merchant logo images only; no PII or transaction data	Tier 2	Ray Yip

Vendor / Partner	Service	Tier	Owner
Redis	Internal real-time notification backbone (Socket.IO); transient event data only	Tier 2	Ray Yip
Day.ai	CRM — sales, onboarding, and implementation pipeline	Tier 2	Kyle Bunbury / Audrey Wilson
Google Workspace	Email, documents, company records	Tier 2	Audrey Wilson
Slack, Zoom	Internal communication, incident channel	Tier 2	Audrey Wilson

5.1 Prospective Partners — Not Yet Under Executed Contract

Prospective Partner	Intended Role	Status
Peoples Trust Company	Sponsor bank / BaaS — settlement, custody, regulated banking functions	**Prospective / pilot-stage**
Innovation Federal Credit Union	Lending partner — underwriting, lending decisions, AML/KYC. Converted to federal charter; likely OSFI-regulated	**Prospective / pilot-stage**
Equifax Canada	Credit-bureau data partner	**Prospective / pilot-stage.** Does not appear among the eleven sub-service organizations in the System Description — confirm whether a bureau integration exists in the current system boundary. *Owner: Ray Yip*

CredX must not describe any of the above as active, contracted relationships.

a. **Current status: no SLA is on file for any vendor in this register, and support and escalation contacts remain to be collected.** Completing the register is a tracked action item owned by the Operations & Compliance Lead. This policy states required practice; the register is not yet evidence of it.

6 Requirements Specific to CredX's Vendor Profile

a. **Pre-execution due diligence.** A security and privacy due-diligence questionnaire must be completed before executing the Peoples Trust Company, Innovation Federal Credit Union, and Equifax Canada agreements, confirming data-handling, security, and regulatory posture — including OSFI-related expectations given Innovation Federal Credit Union's conversion to federal charter status. An annual security review cadence must be established for existing vendors (Clover, Square, Twilio, SendGrid, Ownest). **Neither is yet formalized as a required gate or recurring process. [TBD]**

b. **Contract terms that must be negotiated before execution.** No sponsor bank, lending partner, or merchant agreement currently executed contains data-breach liability, indemnification, or notification-sequencing terms. This is a **Critical** risk. Before any such agreement is signed, it must define:

   i. Which party leads the RROSH determination, and the process for sharing findings.

   ii. The notification sequencing and fixed notice windows across the partner chain (recommend 1–24 hours for anything touching financial or personal data).

   iii. Indemnification scope and caps by layer.

   iv. Incident-coordination obligations, including the partner's own regulatory clocks.

c. **OSFI-regulated partners.** CredX must confirm whether Peoples Trust Company and Innovation Federal Credit Union are OSFI-regulated and, where they are, build their **24-hour** incident reporting obligation into CredX's internal escalation SLA. A partner's regulatory clock is materially faster than CredX's own, and CredX must not become the bottleneck in it.

d. **Technology licensing continuity.** CredX licenses its core technology from Ownest Inc., which retains ownership. Loss of access to that relationship, the source code, or vendor support would halt product development and could impact live decisioning. CredX must establish a technology continuity safeguard:

   i. Source-code or technology escrow held by a neutral third party, releasable on defined trigger events (licensor insolvency, extended unavailability, contract termination); or

   ii. A documented technical handover and transition plan; or

   iii. Contractual continuity and support-SLA terms.

This is a Tier 1 governance action item owned jointly by the CEO and legal counsel, and is **currently unmitigated**.

e. **Platform independence.** Where contractually and technically permitted, CredX must maintain its own export or backup of critical decisioning and merchant data outside the Base44 environment, to avoid single-vendor lock-in risk.

f. **AI and model providers.** Any third-party model or scoring service in the decisioning path is a Tier 1 vendor, and the provider's own model documentation and fairness evidence must be obtained. See the Artificial Intelligence Governance Policy.

g. **Sub-processor disclosure.** Vendors processing personal information on CredX's behalf must be recorded in CredX's sub-processor disclosures under the Privacy Management Policy, and must sign a Data Processing Agreement.