CredX System Description

CredX Tech Inc

September 2026

Contents

Table 1: Document history

Date	Comment
Sep 3 2026	Rewritten for the embedded lending platform
Sep 4 2026	Replaced with SOC 2 System Description v1.0
Sep 4 2026	Verified against source repositories
Sep 4 2026	Recorded confirmed at-rest encryption and S3 residency

1 Purpose and Scope

This System Description is the central narrative in CredX Tech Inc.'s System and Organization Controls (SOC 2) narrative set. It synthesizes and cross-references six companion narratives — the Organizational Narrative, Products and Services Narrative, Control Environment Narrative, Security Architecture Narrative, System Architecture Narrative, and Business Continuity Plan Narrative — into the single, formal description of the system customarily presented as Section III of a SOC 2 report.

It describes, in the terms expected by the AICPA's Description Criteria: the boundaries of CredX's system; the principal service commitments and system requirements CredX has established; the infrastructure, software, people, processes, and data that constitute the system; the sub-service organizations the system relies on; and the known limitations relevant to a reader's understanding.

Scope: the Trust Services Criteria for **Security, Availability, and Confidentiality**.

Certification status: CredX is **not** SOC 2 certified. CredX is pursuing a SOC 2 Type I examination first — a point-in-time assessment of whether controls are suitably designed — followed by a Type II examination covering operating effectiveness over a review period. This document does not itself constitute a SOC 2 report and does not represent that CredX has completed or passed an examination of any type.

2 Overview of the Company and Its Services

CredX Tech Inc. is a pre-revenue financial technology company headquartered in Calgary, Alberta, Canada, at Suite 159 #406, 917-85 St SW, Calgary, AB T3H 5Z9.

CredX operates an **Embedded Value Platform (EVP)**: closed-loop embedded payments, credit decisioning, and merchant lending infrastructure connecting merchant point-of-sale (POS) systems to credit and lending partners.

CredX is a **non-bank technology provider**. It does not hold a banking, money services business, or lending licence, and does not itself perform settlement, custody, underwriting, or AML/KYC functions. Those regulated functions are performed by CredX's sponsor bank, processor, and licensed lending partners. CredX supplies the technology, data orchestration, and integration layer that binds these parties together around a merchant transaction.

2.1 The Six Product Pillars

Pillar	Description
Cost Reduction	Interchange savings for merchants

Pillar	Description
BoosT	Embedded, unsecured buy-now-pay-later and point-of-sale lending. Short for *Balance Offset & Organic Spending Trigger*
Data as a Product	A tokenized, consented transaction-data catalogue, referred to internally as *DaaP*
Marketing	Event-driven, self-funded merchant marketing
MarketPlace	A curated partner ecosystem
Orchestration	A rules engine / policy-as-code layer binding lending policy, customer profiling, consents, and disclosures

CredX refers to the combined structural outcome of these pillars internally as **"MoaT."** Full detail on each pillar is in the Products and Services Narrative.

2.2 Geographic Footprint

CredX's go-to-market is **Canada-first**, with U.S. expansion planned but not yet underway. The platform is presently **CAD-only with no multi-currency support**. Target merchant segments range from MVP (under $12M revenue) through Small, Medium, and Large tiers, across priority industries including grocery, telecom, professional sports, entertainment and venues, utilities, fintech, POS technology partners, and consumer delivery.

3 Principal Service Commitments and System Requirements

These commitments are drawn from CredX's Security Requirements Specification and Data Security & Privacy Policy, and are the standard against which the system requirements and controls described throughout this narrative set are designed.

3.1 Commitments Regarding Security

- Protect the confidentiality, integrity, and availability of merchant, partner, and consumer data, using defense-in-depth controls appropriate to CredX's current stage and scaling toward enterprise/regulated-grade deployment without requiring re-architecture.
- Encrypt data in transit using TLS 1.2 or higher across all client, merchant, and partner connections, with certificate pinning on mobile clients and rejection of weak or deprecated ciphers.
- Encrypt sensitive data at rest using AES-256 or stronger. **Storage-layer encryption at rest is confirmed** across Heroku Postgres and AWS S3.

The specified field-level encryption for high-risk PII attributes is not implemented, and two known exceptions are named in Known System Limitations below.
- Authenticate and authorize all administrative and API access using role-based access control (RBAC) and multi-factor authentication (MFA) for administrative and operational accounts, with least-privilege provisioning and audited admin actions.
- Protect the in-store payment credential — the dynamic QR/barcode presented from Apple Wallet or Google Wallet — using time-bound, single-use, cryptographically signed tokens designed to resist screenshot, replay, and reuse.

3.2 Commitments Regarding Availability

- Maintain availability for order intake, merchant notification, and QR-based payment validation through rate limiting, DDoS protection, automated health checks and restarts, and regularly tested backups.
- Isolate development, staging, and production environments so that non-production activity cannot degrade production availability.

3.3 Commitments Regarding Confidentiality

- Confine PII and payment-related workloads to infrastructure located in Canada, supporting data residency and sovereignty expectations under Canadian privacy law.
- Limit the customer data shared with sub-service organizations to the minimum required for each integration to function, and **never transmit applicant financial data to Ownest via API — only a correlation/loan identifier**.
- Apply CredX's PII classification scheme (Public, Internal, Confidential, Restricted) and data-minimization principles grounded in Privacy by Design, consistent with Alberta's Personal Information Protection Act (PIPA) and the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

3.4 System Requirements Derived From These Commitments

Requirement Area	Specified Requirement	Status
Transport encryption	TLS 1.2+ on all connections; certificate pinning on mobile clients; weak/deprecated ciphers rejected	Specified; production configuration to be verified prior to audit fieldwork

Requirement Area	Specified Requirement	Status
Encryption at rest (storage layer)	AES-256 or stronger for data at rest	**Confirmed** — platform-managed encryption on Heroku Postgres and AWS S3 (`ca-central-1`)
Encryption at rest (application layer)	Field-level encryption for high-risk PII attributes	**NOT implemented** — no encryption primitive exists in the codebase; see named exceptions below
Payment credential	Dynamic, rotating, time-bound QR/barcode (TTL 30–60 seconds), HMAC-signed, invalidated after scan	Specified; production behavior to be confirmed
Access control	RBAC, least privilege, MFA on admin/operational accounts, audited admin actions	Specified; production enforcement to be verified prior to audit fieldwork
Data residency	PII and payment workloads confined to Canadian infrastructure	**Implemented** — Heroku Private Spaces (Canadian region) for the application and database; AWS S3 in `ca-central-1` for merchant logo storage
Monitoring / alerting	Continuous monitoring and automated alerting on suspicious QR/API activity	**NOT yet implemented** — named gap

4 System Boundaries

Defining the boundary of the system establishes which components, processes, and controls are within CredX's own audit scope, and which belong to other parties whose controls CredX relies upon but does not control.

4.1 In Scope

- CredX's backend API services and orchestration/data layer, including order intake, merchant notification, wallet credential issuance and validation, loan draw-down recording, and POS reconciliation logic.
- CredX's iOS and Android mobile applications, including wallet-pass issuance and QR/barcode display logic.
- CredX's digital wallet integration layer — the code and configuration CredX controls for Apple Wallet and Google Wallet pass issuance and updates — but not Apple's or Google's own wallet platforms, which are

carve-out sub-service organizations.
- CredX's real-time notification layer — the websocket channel backed by Redis, and CredX's use of the managed push service — to the extent it is CredX-operated configuration rather than the underlying third-party service.
- CredX's own infrastructure environment: Heroku Private Spaces (Canadian region) as configured and administered by CredX, including environment isolation between development, staging, and production.
- CredX's internal governance, access control, and incident response processes as they apply to the components above.

4.2 Out of Scope (Carved Out)

- The sponsor bank's core banking systems, ledgers, and settlement infrastructure. Sponsor bank relationships (Peoples Trust Company, Innovation Federal Credit Union) are **prospective/pilot-stage and not yet under executed contract**.
- Lender underwriting systems operated by Ownest Inc., including the UnderwriteFlow decisioning application and Ownest's hosted questionnaire flow. CredX does not transmit applicant financial data to Ownest via API and does not operate or control Ownest's underwriting infrastructure.
- POS partners' own systems and infrastructure (Clover, Square), including their payment-tender processing, data stores, and security controls.
- Payment network rails and card-network processing occurring once a transaction leaves CredX's and the POS partner's systems.
- All other sub-service organizations listed below — their internal controls are outside CredX's system boundary and are addressed using the carve-out method.

This boundary is drawn consistently with CredX's regulatory posture: CredX is not a bank, not a FINTRAC-registered Money Services Business, and does not independently perform KYC/KYB. Those functions, and the systems that perform them, sit outside CredX's system boundary by design.

5 Infrastructure

CredX's backend is hosted on **Heroku Private Spaces, provisioned in a Canadian region**, selected specifically to support Canadian data residency. CredX confines all PII and payment-related workloads to the Canadian Private Space.

This is a verified, current fact and **supersedes any earlier reference to AWS hosting** that may appear in older marketing materials. Heroku Private Spaces, Canadian region, is the authoritative infrastructure fact for this narrative set.

Data stores. The system of record is a **PostgreSQL** database hosted alongside the application in the Canadian Private Space, with platform-managed AES-256

encryption at rest. **AWS S3 in `ca-central-1`** stores merchant logo images only and holds no PII or transaction data. Both regions keep data within Canada, supporting the residency commitment above.

Environment isolation. Development, staging, and production environments are separated using separate Heroku Private Spaces or, where a separate Private Space is not used, strict network segmentation.

Network controls. Backend traffic is HTTPS-only (Heroku SSL). Inbound traffic is intended to be restricted using IP allowlists, private networking, or internal routing; production configuration of these controls should be verified prior to audit fieldwork.

Application and data model. The backend is organized into discrete functional domains — merchant onboarding, order intake, wallet and credential issuance, and loan and transaction processing. The data model is defined declaratively and version-controlled, providing a single source of truth for the database structure. This narrative describes the data model at a functional level only and does not disclose schema internals, credentials, or infrastructure configuration detail.

Secrets management. Secrets — API keys, encryption keys, and signing secrets — are to be held only in the platform's managed configuration store or an approved secrets manager, with regular rotation, per-environment separation, and no secrets committed to source control. Production adherence should be confirmed prior to audit fieldwork; one known exception is named below, where this control did not hold for POS integration credentials.

6 Software

6.1 Client Applications

CredX's client estate comprises four applications, not the single consumer mobile application described in earlier drafts:

- **Consumer web application** — the customer-facing experience: credit application flow, wallet and payment-credential presentation, scanning, transaction history, and profile. It is a **web** application, not a native mobile app.
- **Merchant mobile application** — iOS and Android; order queue and in-store scanning. Receives push and real-time order alerts, and uses platform-backed secure storage for local secrets.
- **Administrative dashboard** — internal use over the platform API.
- **POS device application** — a native application deployed to Clover point-of-sale hardware. **This component appears in no prior compliance documentation** and should be assessed for inclusion in, or explicit carve-out from, the system boundary.

Digital wallet integration is implemented for **both** providers — Apple Wallet via PassKit, Google Wallet via service-account authentication. CredX issues wallet passes whose face displays **only the merchant name** — no balance or credit limit is shown — and whose barcode is a dynamic, rotating, time-bound code functioning as the in-store payment credential.

6.2 Backend API Services

The backend is a TypeScript service exposing a **GraphQL** API, backed by **PostgreSQL** and **Redis**, deployed in Heroku Private Spaces in the Canadian region. Database migrations are applied automatically on release.

It provides merchant onboarding and POS connection, webhook intake from POS providers, wallet-pass issuance and credential validation, and loan, transaction, and ledger processing. Merchants authenticate their own software integrations using a merchant-specific API key; **these keys are stored as salted hashes**, alongside a short non-secret prefix used for lookup.

6.3 Real-Time Notification Layer

CredX operates two real-time channels for merchant-facing and transaction events: a **websocket channel**, backed by Redis, as the real-time notification backbone; and a **managed mobile push service**, for merchant device order alerts carrying order identifier, merchant, location, and total — deliberately excluding customer data from this event.

Known exception. Payment-confirmation push notifications are **disabled**. The push service is specified in the architecture to deliver payment-confirmation notifications alongside order alerts, but that path is currently switched off. Payment confirmation today relies solely on the real-time websocket channel, with no fallback if that connection drops.

7 People

CredX is a small, pre-revenue company, and its people-related controls are sized accordingly. Work is organized into **four functional areas — Leadership, Sales, Operations, and Technical** — each currently staffed by one member of the founding team. Responsibilities throughout this program attach to the function rather than the individual.

Ray Yip, Chief Technology Officer, owns platform administration, security architecture, and infrastructure decisions for the in-scope system, and **also serves as CTO of the affiliated company Ownest Inc.**

The four functional owners — Kendall Raessler (Leadership, Founder & CEO), Ray Yip (Technical, CTO), Kyle Bunbury (Sales, Co-Founder & VP), and Audrey Wilson (Operations, Co-Founder & VP) — also constitute CredX's

Incident Response Team. Because each function is currently a single-person function, CredX names **functional continuity** as a risk and maintains a cross-function cover arrangement: each function has a designated covering function that assumes its responsibilities during an absence, confirmed by the CEO at the point of an incident. Human Resources and Finance are not separately staffed; their responsibilities sit with Leadership and Operations.

CredX **does not yet have a formal board of directors or independent oversight body**. Governance today runs through the leadership team and the Data Security & Privacy Policy's intended joint CTO / Chief Compliance Officer (CCO) oversight model, where the CCO function is presently carried informally by Audrey Wilson under her VP, Operations title.

8 Data

8.1 Categories of Data Processed

Data Category	Examples	Sensitivity
Personally identifiable information (PII)	Name, email address, phone number, government-issued identifiers, device identifiers linked to an individual	Restricted
Financial / transaction data	Order totals, line items, payments, refunds, loan ledger entries	Restricted
Merchant / partner data	Merchant profile data, POS access tokens, merchant logo images, API keys	Confidential
Behavioral / device data	Transaction metadata tied to identifiable users, device identifiers, push/notification tokens	Confidential

CredX applies a four-tier PII classification scheme (Public, Internal, Confidential, Restricted) grounded in Ann Cavoukian's seven Foundational Privacy by Design principles. One open item under this framework — **Principle 7, user-facing consent and access mechanisms** — is not yet confirmed as implemented.

8.2 Transaction Lifecycle

Step	Event	Mechanism
1. Order appears	A POS provider (Clover or Square) creates an order	The provider posts a webhook; the signature is verified, the order fetched back from the provider, and mirrored into CredX's database

Step	Event	Mechanism
2. Merchant device notified	CredX notifies the merchant's device of the pending order	Push and websocket channels carry order identifier, merchant, location, and total — **no customer data in this event**
3. Customer presents pass	Consumer presents their wallet pass in-store	The wallet barcode is scanned and submitted to the backend; the rotating code resolves to a user and an active loan
4. Loan drawn down	CredX records the financing event	Payment, transaction, and ledger entries written atomically together
5. POS reconciled	CredX reconciles the payment back to the POS provider	For Square, a payment collected outside Square's own tender flow is recorded. For Clover, the record is created through a customer-facing tender call and read back to confirm

8.3 Money Data Model

CredX's financial data model is organized around six related record types — **orders, order line items, payments, refunds, transactions, and the loan ledger**. The following integrity controls apply:

- **Precise decimal arithmetic.** Every monetary value uses a fixed-precision decimal type; no floating-point monetary values exist anywhere in the schema.
- **Atomic transactions.** The draw-down path wraps the loan debit — writing both the transaction and the ledger entry — together with the order and payment status updates in a single database transaction, with rollback handling on error.
- **Idempotency keys.** Payments and refunds each carry a unique idempotency key, and both paths return the existing record rather than reprocessing a replayed key.
- **Credential attribution.** Payment and refund records are each stamped with the merchant API credential that authorized them.

Identifier hygiene note. Several record types share a commonly-named external identifier field, each referring to a **different external partner's identifier namespace**. POS order and refund identities are carried by distinctly named fields, so the shared identifier does not span order and payment records. The caution stands: these identifiers are **context-dependent, not globally unique**, and any join or report using one must first establish which partner namespace it refers to.

9 Sub-Service Organizations

CredX relies on **eleven external systems**. Consistent with SOC 2 practice, the controls of carve-out sub-service organizations are not evaluated as part of CredX's own examination; a reader relying on this description should separately consider those organizations' own control assurances.

System	Role	Auth Model	Data Shared by CredX
Clover	POS provider	OAuth v2, auto-refresh + recovery	Merchant and money/order data; no customer PII. Partial refunds on external-tender payments are not supported
Square	POS provider	Static, admin-pasted token	Merchant and money/order data; no customer PII. No refresh/expiry/revocation detection today
Ownest	Credit underwriting (affiliated company)	OAuth client credentials (machine-to-machine)	**Only a correlation identifier — no applicant financial data sent from CredX via API**
Apple Wallet / APNs	Payment instrument (wallet pass + push)	Pass certificates + APNs token auth	User ID travels inside the scannable barcode; merchant name on pass face; no balance/limit shown
Google Wallet	Payment instrument (wallet pass)	Service-account JWT	Same barcode design as Apple Wallet
Sign in with Apple / Google	Customer authentication	JWKS / OAuth2 ID token	Identity assertions used for consumer login
Twilio	SMS (login codes / OTP)	Account SID / token	Phone number, OTP, and message body. **Recipient phone numbers are also written to application logs on every send**
SendGrid	Email (OTP, admin links)	API key	Email address, first name, and OTP/link content
Expo Push	Merchant order alerts	Push token	Device token, merchant and location identifiers, and order total. **Payment-confirmation push is disabled**
AWS S3	Merchant logo storage	Access key	Logo images only — no PII or transaction data

System	Role	Auth Model	Data Shared by CredX
Redis	Real-time notification backbone	Connection URL	Transient real-time event data only; no durable partner data retained

All are treated as carve-outs, except Expo Push, which is partial: the push infrastructure is a carve-out while CredX-side push integration code is in scope.

10 Known System Limitations

Consistent with SOC 2's expectation of a candid system description, CredX documents the following known limitations identified through internal review of its Partner Data Map, data model, and Security Requirements Specification. Each is a tracked item with a remediation owner, not an unmanaged failure. Several are acceptable at CredX's current Canada-only, pre-revenue stage but would need addressing before broader scale, multi-currency expansion, or a Type II examination.

#	Limitation	Practical Impact	Owner
1	Refunds are recorded at amount level, not item level, and the refund reason field is not populated	Reduces granularity of refund reporting and root-cause analysis for partial refunds	Technical function
2	Transaction-to-item traceability requires several relationship hops and is not enforced at the database level	Increases risk of reporting errors if application-layer logic is not applied consistently	Technical function
3	Order quantity cannot express fractions	Fractional or weighted-quantity sales — items sold by weight — are not supported and could fail or be misrecorded	Technical function
4	The data model carries no currency dimension; CAD is assumed	Acceptable while Canada-only; a hard blocker for planned U.S. multi-currency expansion	Technical function — required before U.S. launch
5	The funding lender is not reconciled back onto the loan record; a placeholder reference persists	Limits accurate reporting on which lender funded a given loan without manual cross-reference	Technical function

#	Limitation	Practical Impact	Owner
6	Integration and webhook failures — POS token refresh failures, rejected webhooks, failed provider calls — are not written to the audit log, only to shorter-retention application logs	Reduces auditability and retention of integration failure history relative to stated logging requirements	Technical function
7	**Stored POS integration credentials and the wallet-pass rotating-code secret are held unencrypted.** Storage-layer encryption at rest is confirmed, but these are unencrypted values *inside* the encrypted database — readable by anything with query access, so platform encryption does not mitigate them. No encryption primitive exists anywhere in the backend. (Merchant API keys, by contrast, are salted-hashed.)	**Top-priority open remediation item. See limitation 11 — the exposure is not limited to database compromise**	**Technical function — top priority**
8	Square's integration uses a static administrator-supplied token with no refresh, expiry, or revocation detection	A revoked or rotated token may not be detected promptly, risking silent integration failure or continued use of an invalid credential	Technical function
9	Payment-confirmation push notifications are disabled; confirmation relies solely on the websocket channel	Reduces redundancy of the payment-confirmation notification path	Technical function
10	No live monitoring or SIEM capability exists today (NIST CSF 2.0 "Detect" scored 0 of 4)	Suspicious activity, anomalies, or intrusions would not currently be detected in real time by an automated system	Technical function — Phase 2 of the Layered Security Roadmap

#	Limitation	Practical Impact	Owner
11	**The stored POS credential is exposed as an API field, and the single-merchant lookup enforces authentication but not role authorization** — unlike every sibling merchant operation, which is administrator-only. The lookup applies no field selection	**Any authenticated user of any role, including an ordinary consumer, can retrieve a merchant's live POS access credential through the API.** This escalates limitation 7 from a database-compromise scenario to a live authorization defect	**Technical function — Critical**
12	**The POS device application is undocumented**	A deployed component of the estate sits outside every system boundary description, sub-service inventory, and security assessment	**Technical function**

Target dates for all items are [TBD]. Limitations 1–10 were carried from CredX's internal review and re-confirmed; limitations 11 and 12 were identified during that review.

CredX's position is that naming these items explicitly — rather than omitting or softening them — is necessary for the credibility of this narrative set, since an auditor performing walkthroughs or code-level review would identify them regardless.

11 Outstanding Inconsistencies Across Source Documents

Two conflicts exist between CredX's own current source documents and should be resolved before this narrative set is issued externally.

BoosT unsecured lending ceiling The System Description states a **$25,000** unsecured lending ceiling; the Products and Services Narrative states **$5,000 per consumer**. These cannot both be correct. *Owner: Kyle Bunbury / Kendall Raessler.*

Merchant onboarding model The Products and Services Narrative describes MVP and Small tier merchants onboarding through a **self-serve merchant portal**; the System Architecture Narrative states merchants onboard **internally, not via a self-serve public flow**. *Owner: Kyle Bunbury / Ray Yip.*

A third item to confirm: **Equifax Canada** appears in the Control Environment Narrative as a prospective/pilot-stage credit-bureau data partner, but does not appear among the eleven sub-service organizations above. Confirm whether a bureau integration exists in the current system boundary. *Owner: Ray Yip.*

12 Changes to the System Since the Prior Period

This is the first SOC 2 narrative prepared by CredX. There is no prior-period system description against which to report changes, and this section is therefore **Not Applicable** for a pre-audit baseline. This document establishes the starting point from which future period-over-period reporting will be measured.