Security Incident Response Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.3, CC7.4, CC7.5

Table 2: Document history

Date	Comment
Nov 28 2024	Updated document structure
Sep 3 2026	Added severity levels and breach notification chain

1 Purpose and Scope

1.1 Purpose

This Security Incident Response Policy establishes controls to ensure the timely detection and response to security incidents and vulnerabilities. It provides clear guidelines for incident reporting, classification, investigation, resolution, and communication.

1.2 Scope

This policy applies to all users of CredX's information systems, including employees, contractors, and external parties with system access. All users must adhere to this policy to maintain the security and integrity of CredX's information assets.

2 Background

CredX is committed to detecting and mitigating information security risks to protect employees, customers, and partners. Security incidents, including data breaches, must be promptly addressed to minimize damage and legal exposure. This policy ensures a structured approach to incident management.

3 Policy

3.1 Reporting Incidents

- All users must report suspected or confirmed security incidents **immediately** — and in no case later than 24 hours — to the Technology & Infrastructure Lead (Ray Yip, CTO). For suspected security or data incidents, the Operations & Compliance Lead (Audrey Wilson) must be notified **in parallel**, not sequentially.
- The Slack incident channel is the primary reporting and coordination channel. A phone/SMS tree is the backup if Slack itself is unavailable.
- CredX's regulated partners operate on materially faster regulatory clocks than CredX's own. An OSFI-regulated banking or lending partner must report a technology or cyber security incident within **24 hours**. CredX's internal detection-to-decision process must therefore be fast enough not to become the bottleneck in a partner's regulatory deadline.
- Failure to report security incidents will result in disciplinary action.

3.2 Incident Handling

- All security incidents must follow the defined incident management procedures.
- Incident response procedures must be reviewed and updated annually.
- Incident response testing must be conducted at least twice per year.
- Incident logs must be reviewed monthly to assess response effectiveness.

3.3 Data Preservation

- Evidence related to security incidents (e.g., logs, files, system snapshots) must be preserved for investigation and potential legal proceedings.

4 Procedure for Establishing Incident Response System

4.1 Designation of Roles

The Incident Response Team is drawn from CredX's leadership team given the company's small size:

Role	Name	Responsibilities
Incident Commander / Executive Escalation	Kendall Raessler — Founder & CEO	Final decision authority during a declared incident; owns external stakeholder, investor, and partner-bank communication; approves activation and deactivation
Technology & Infrastructure Lead	Ray Yip — CTO	Technical assessment, severity assignment, containment, system restoration, hosting/vendor escalation, data recovery
Sales & Partner Continuity Lead	Kyle Bunbury — Co-Founder & VP, Sales	Communication continuity with merchant and lender pipeline; CRM data recovery
Operations & Compliance Lead	Audrey Wilson — Co-Founder & VP, Marketing & Operations	Breach notification coordination, regulatory notification tracking, compliance documentation, internal staff communications

- Contact details, including designated backups, are held in Appendix A of the Disaster Recovery Policy and in a secure contact sheet stored outside systems that could themselves be affected by an incident.
- **Functional unavailability is a named High risk.** Each function is currently staffed by one person. Cover is assigned by function — Operations

covers Leadership and Sales, Technical covers Operations, and Operations plus a contracted engineer covers Technical — and the CEO confirms cover at the point of an incident. CredX is too small to operate a rotating on-call schedule; this cross-function arrangement substitutes for one.

- Legal counsel is engaged for any suspected personal data breach and for any incident implicating partner agreements.

4.2 Communication Channels

- A dedicated security incident email inbox must be monitored for reports.
- An incident ticketing system must be used for tracking incidents.
- Updated contact details for the on-call ISM must be maintained.

4.3 Training and Awareness

- All employees must complete security incident response training twice annually.
- Incident response procedures must be accessible to all users.

5 Procedure for Executing Incident Response

5.1 Incident Identification

- Users must report incidents within 24 hours to their manager, who must escalate it to the ISM.
- Reports must include:
  - Incident description
  - Date, time, and location
  - Reporting person
  - Evidence and affected systems

5.2 Incident Investigation

- The Technology & Infrastructure Lead assesses scope and assigns a severity level within the target response windows below:

Severity	Definition	Example	Activation
P1 — Critical	Full outage of Tier 1 system(s); customer/partner-facing impact; potential data exposure	Decisioning platform down; suspected breach	Immediate — Incident Commander (CEO) notified within **30 minutes**; full DR Plan activated
P2 — High	Partial outage or degraded Tier 1 system; single vendor/integration down	Ownest decisioning unavailable; one POS integration failing	Technology Lead activates response within **2 hours**; CEO briefed same day
P3 — Medium	Tier 2 system disruption; limited operational impact	CRM outage, internal tool disruption	Owning lead manages; resolve within target RTO; report at next leadership sync
P4 — Low	Tier 3 or minor issue; no customer/partner impact	Marketing site down	Handled as a routine IT ticket

5.3 Criteria and Response Times for Merchant and Partner Notification

- Merchants and partners must be notified of incidents based on the classification:
  - **P1 — Critical:** Notified within 24 hours of incident confirmation.
  - **P2 — High:** Notified within 48 hours of incident confirmation.
  - **P3/P4:** Notified within 72 hours if their data or operations are affected.
- The Operations & Compliance Lead drafts, and the Incident Commander approves, any communication to merchants, lenders, or sponsor-bank partners. Communications must be factual, avoid speculation on cause until confirmed, and provide a clear next-update time.
- **Only the Founder & CEO, or their explicit delegate, may speak publicly or to media about an incident.**
- Notifications must include:
  - Summary of the incident
  - Impact assessment
  - Mitigation steps taken

– Further actions required, if any

5.4 Regulatory and Legal Notification

- In the event of a personal data breach (unauthorized access to, disclosure of, or loss of personal information), the Operations & Compliance Lead must begin the assessment immediately and **in parallel** with technical containment — not after recovery completes.
- 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 for CredX given merchants and processors located outside Alberta. In practice CredX must meet both standards, which are substantively similar.
- The applicable notification timelines are:

Law / Regulator	Applies To	Trigger	Notice Timing	Individual Notice
Alberta PIPA (OIPC Alberta)	CredX's Alberta operations	RROSH	Without unreasonable delay — in practice **days, not weeks**	Mandatory, direct
PIPEDA (OPC Canada)	Interprovincial / cross-border handling	RROSH	As soon as feasible after the breach is determined	Mandatory, direct
Both PIPA and PIPEDA	All breaches, regardless of RROSH	Any breach of security safeguards	No deadline, but a record of **every** breach kept **24 months** and produced on request	N/A
OSFI Technology and Cyber Security Incident Reporting Advisory	Federally regulated banking/lending partners	Reportable technology or cyber incident	**Within 24 hours**, sooner if possible	N/A (institution to regulator)

Law / Regulator	Applies To	Trigger	Notice Timing	Individual Notice
PCI DSS (contractual, not statutory)	Any party handling cardholder data, including merchants	Suspected or confirmed cardholder data compromise	Immediate notice to acquiring bank/processor	N/A

- A **24-month breach record log** must be maintained for every breach of security safeguards, regardless of whether RROSH was determined and regardless of whether notification was required.
- A documented **RROSH assessment procedure** with a named owner and a fixed internal SLA must be followed for each incident involving personal information.
- Affected individuals must be notified where RROSH is established.
- All regulatory notifications must be documented, including the decision rationale if notification was deemed unnecessary. Breach reports must match the OIPC/OPC prescribed fields: organization contact, breach description and cause, dates, data categories, number affected, and mitigation steps.
- Engage legal counsel immediately upon suspected breach to assess obligations and applicable timelines. This policy does not constitute legal advice.

5.5 Notification Chain Across the Partner Chain

Because the same underlying data can touch CredX's platform, a bank or lender's systems, and merchant records, breach notification runs across a chain. **No notification-chain protocol currently exists in any executed CredX agreement** — this is a Critical risk in the Risk Register, and the sequence below is the standard CredX must negotiate into partner and merchant agreements before execution.

1. **Detection & immediate internal notice** — whichever party (CredX, sponsor bank, or lending partner) detects the incident notifies the others within a contractually fixed window (recommend 1–24 hours for anything touching financial or personal data), **independent of whether RROSH has been determined yet**.
2. **Joint RROSH assessment** — the relevant partner agreement should designate a lead for the RROSH determination and a process for shar-

ing findings, since each entity carries an independent regulatory notice obligation.

3. **Parallel regulator notice** — each entity notifies its own regulator directly and simultaneously: CredX to OIPC Alberta (and OPC, where cross-provincial data is involved); a federally regulated bank or lender to OSFI. **Entities do not wait on each other to start their own clock.**
4. **CredX notifies affected merchants** — without unreasonable delay once RROSH is confirmed for data touching their business, mirroring the PIPA standard CredX is itself held to.
5. **Merchant notifies their own customers and insurer** — the merchant's independent obligations begin running from their own discovery or notice from CredX. CredX notifying the merchant does **not** discharge the merchant's own duty to their end customers.

5.6 Liability Allocation by Layer

Regulators have consistently held that performance can be delegated but regulatory accountability cannot: whatever a technology provider does on a regulated partner's charter is treated by regulators as if the regulated partner did it directly. Indemnification clauses shift financial responsibility between parties after the fact; **they do not shift regulatory findings.**

Banking / lending partner (Peoples Trust, Innovation FCU)

- *Regulatory accountability:* retains ultimate accountability for compliance failures tied to their charter — AML/KYC, consumer protection, lending decisions — **even where CredX's technology caused the incident**.
- *Contractual/financial liability:* will typically seek indemnification from CredX for costs traceable to CredX's platform.
- *Status at CredX:* **not yet executed — priority contract term.**

CredX (technology / platform layer)

- *Regulatory accountability:* not directly regulated as a bank or MSB, but accountable for its own privacy-law obligations under PIPA/PIPEDA **as the entity controlling personal information on its platform** — including where the checkout carries the merchant's brand.
- *Contractual/financial liability:* should expect to carry financial exposure for platform-caused incidents, ideally capped through negotiated indemnification limits.
- *Status at CredX:* **indemnification caps not yet negotiated — priority contract term.**

Merchant

- *Regulatory accountability:* accountable for their own PCI DSS compliance and their own downstream customer notice and insurance obligations.

- *Contractual/financial liability:* generally not liable for a breach occurring inside CredX's or the partner bank/lender's systems, unless caused by the merchant's own negligence — for example, compromised POS credentials.
- *Status at CredX:* **not yet defined in a standard Merchant Network Agreement.**

5.7 Merchant Obligations to Insurers and Customers

- **Insurer notice**: most commercial and cyber insurance policies require notice "as soon as practicable," commonly within 24–72 hours of the merchant's own discovery. Missing this window is a common reason insurers reduce or deny claims.
- **Customer notice**: where the merchant controls personal information about its own customers, it carries an independent RROSH-triggered obligation under PIPA/PIPEDA or applicable provincial law.
- **PCI DSS**: if cardholder data is implicated, the merchant must notify their acquiring bank or processor immediately upon discovery, and may be required to engage a PCI Forensic Investigator.
- CredX should commit contractually to supplying merchants with the following promptly enough that merchants can meet their own insurer's notice window — recommended as a specific Merchant Network Agreement clause:
  - Date and time of discovery
  - Nature and root cause, if known
  - Categories and volume of personal or cardholder data affected
  - Containment and mitigation steps taken
  - Whether law enforcement or a regulator has been notified
  - Forensic investigation findings, if any
  - Copies of any notices already sent to affected individuals or regulators

5.8 Cyber Insurance Notification

- When any senior executive officer becomes aware of a cyber incident or any event that may reasonably give rise to an insurance claim, CredX's cyber insurer must be notified as soon as reasonably practicable. For cyber incidents, notification may be made by calling the insurer's 24/7 cyber incident response line.
- In the event of cyber crime (e.g., funds transfer fraud, social engineering) or a cyber extortion demand, the incident must also be reported to appropriate law enforcement authorities as soon as reasonably practicable.
- **Ransom payments must not be made without the cyber insurer's prior written agreement.** No costs, ransom payments, or settlement commitments may be made without the insurer's prior written consent,

except that necessary costs incurred within the first **72 hours** of discovering a cyber event may be authorized without prior written consent. Any third-party vendors engaged within this 72-hour window must be drawn from the insurer's approved claims panel providers.

- The Operations & Compliance Lead is responsible for maintaining current contact details for the cyber insurer's claims manager and incident response line, and for ensuring these are accessible during an incident.
- **Cyber insurance coverage is not yet confirmed at CredX. [TBD]** Until it is, this section describes intended practice rather than an available response option, and no reliance should be placed on insurer-funded incident response.

5.9 Four-Phase Response Structure

CredX's incident response is structured around four phases.

Phase 1 — Preparation. Keep this policy, the Risk Register, and the Incident Response Team contact sheet current at all times. The Technology & Infrastructure Lead and a designated backup maintain ready access to the Ownest platform admin console, Day.ai CRM, Google Workspace admin, and POS partner portals (Clover, Square). All team members know the reporting channel and their role. *The tabletop exercises required below have not yet been conducted — preparation is therefore documented but untested.*

Phase 2 — Detection & Analysis. Any team member identifying a potential incident notifies the Technology & Infrastructure Lead and, for suspected security or data incidents, the Operations & Compliance Lead in parallel. The Technology Lead assesses scope and assigns a severity level within the target response windows. *Note that no live monitoring or alerting tooling is confirmed in production, so detection currently depends on human observation and partner status pages.*

Phase 3 — Containment, Eradication & Recovery.

1. **Activation** — For P1/P2 incidents, the Incident Commander is notified and formally activates the Disaster Recovery Plan. The Incident Response Team convenes (video call acceptable) to confirm roles and next steps.
2. **Containment** — The Technology Lead takes immediate action to limit damage or spread **before full root cause is known**: revoking compromised credentials, pausing affected integrations, isolating affected systems, revoking tokens, and disabling QR functionality.
3. **Communication** — Execute the notification requirements of this policy: internal staff, affected merchants and partners, regulated partners, and — where a personal data breach is confirmed or suspected — the breach notification protocol begins **immediately and in parallel**.
4. **Recovery** — Restore systems and data per the Disaster Recovery Policy, prioritized by criticality tier and RTO target.

5. **Validation** — The Technology Lead confirms restored systems function correctly and data integrity is verified before declaring recovery complete.

Phase 4 — Post-Incident Activity. The Incident Commander formally deactivates the plan once normal operations resume, and the post-incident review below is completed.

5.10 Incident Containment and Resolution

- The Technology & Infrastructure Lead, in consultation with the Incident Commander, determines appropriate containment and remediation actions.
- Containment actions may be taken before root cause is established. Speed of containment takes precedence over completeness of diagnosis for P1 and P2 incidents.
- If the incident is categorized as P1 or P2, a communications plan must be developed by the Operations & Compliance Lead and approved by the Incident Commander, with legal counsel engaged where personal data or partner agreements are implicated.
- The Technology & Infrastructure Lead must ensure preservation of forensic evidence for law enforcement if required.
- Actions taken to mitigate the incident must be logged, including:
  - Description and severity
  - Root cause
  - Mitigation steps
  - Disclosure recipients (e.g., customers, vendors, regulators)

5.11 Post-Incident Review

- A post-mortem analysis must be conducted within **5 business days** of incident closure to identify root causes and improvements.
- The post-mortem must document:
  - Incident summary
  - Timeline of events
  - Root cause analysis
  - Systems and data affected
  - Containment and remediation actions taken
  - Effectiveness assessment
  - Gaps identified in detection or response

  - Corrective actions with named owners and due dates
  - Resulting updates to this policy and to the Risk Register
- Lessons learned must be shared across the organization within 10 business days of closure.
- The CEO may escalate serious incidents to external authorities, including law enforcement and regulatory bodies.

5.12 Incident Response Testing

- The incident response plan must be tested at minimum **twice per year** (recommended Q1 and Q3) via a tabletop exercise involving the full Incident Response Team, walking through at least one scenario from the Risk Register.
- **No tabletop exercise has yet been conducted.** This is why the NIST CSF "Respond" function is scored 2 — Developing rather than higher, and scheduling the first exercise is a tracked action item.
- Test results, findings, and action items must be documented and used to update the incident response plan within 30 days of the exercise.
- Ad hoc or simulated incident exercises (e.g., phishing simulations, breach scenarios) are encouraged throughout the year in addition to the formal annual exercise.

5.13 User Notifications and Remediation

- Users must be informed of incidents affecting them.
- Additional training must be provided if necessary.
- Disciplinary actions must be taken if malicious intent is detected.