Disaster Recovery Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	A1.2, A1.3

Table 2: Document history

Date	Comment
Jan 1 2023	Updated contact info
Jan 10 2025	Updated contact info
Sep 3 2026	Added tiered recovery objectives and severity levels
Sep 4 2026	Recovery objectives validated; backup policy confirmed

1 Purpose and Scope

a. The purpose of this policy is to define CredX's procedures to recover Information Technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident. The objective of this plan is to complete the recovery of IT infrastructure and IT services within the Recovery Time Objectives (RTOs) set out below.

b. This policy includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management.

c. This policy applies to all management, employees and suppliers that are involved in the recovery of IT infrastructure and services within CredX. This policy must be made readily available to all whom it applies to.

d. This policy operates alongside the Business Continuity Plan, which holds the business impact analysis, the critical vendor register, and the wider continuity strategy.

2 Background

a. This policy defines the overall disaster recovery strategy for CredX. The strategy describes CredX's Recovery Time Objectives and Recovery Point Objectives by criticality tier, as well as the procedures, responsibility and technical guidance required to meet them.

b. The following conditions must be met for this plan to be viable:

   i. All software and data (or their backups/failovers) are available in some manner.

   ii. Resources involved in recovery efforts can work from an alternate location. CredX is a remote-capable team, so workspace disruption alone is a Low-rated risk.

   iii. The Information Security Manager is responsible for coordinating and conducting a rehearsal of this plan at least twice per year.

c. This plan does not cover the following types of incidents:

   i. Incidents that affect merchants or partners but have no effect on CredX's systems; in this case, the merchant or partner must employ their own continuity processes.

   ii. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Heroku and the Ownest/Base44 decisioning environment. CredX depends on such suppliers to employ their own continuity processes.

iii. Security incident response procedures of CredX's sponsor bank, processor, or lending partners, who retain responsibility for their own regulated infrastructure. Coordination with those partners is governed by the Security Incident Response Policy.

3 Known Limitations

a. This policy states its requirements as CredX intends to operate them. The following are **not yet in place**, and this policy should not be read as evidence that they are:

   i. Multi-region or failover redundancy within Heroku Private Spaces is not confirmed.

   ii. **No restore test has been performed against production backups.** The backup policy is confirmed and the recovery objectives are validated, but neither has been demonstrated by an actual restore.

   iii. Written backup, redundancy, and SLA documentation has not been obtained from Ownest for the Base44-hosted decisioning environment.

   iv. No live monitoring or alerting tooling is confirmed in production, so detection of a disaster depends on personnel observation and partner status pages.

   v. **The recovery objectives in this policy are validated but not yet tested.** They have been reviewed and confirmed as achievable against the Heroku Private Spaces (Canadian region) environment. **No restore or failover has yet been performed and timed against them**, so they are a validated design rather than demonstrated recovery capability.

   vi. Because the NIST CSF "Detect" function is scored 0 of 4, detection capability and recovery-time measurement are linked: **without reliable detection, the clock on an actual recovery event is harder to start accurately**, which is a further reason formal RTO/RPO validation remains pending.

b. Closing these gaps is tracked in the Business Continuity Plan's open action items. Until they are closed, CredX must not represent its recovery capability as tested.

4 Policy

a. *Recovery Objectives*

   i. Systems are assigned a criticality tier: **Tier 1 (Critical)** — customer/partner-facing, revenue- or compliance-impacting; **Tier**

2 (Important) — internal operations, degrades service if down more than 24 hours; **Tier 3 (Low)** — non-essential, marketing or back-office.

ii. The recovery objectives below have been reviewed against the confirmed Heroku Private Spaces (Canadian region) environment. They are the documented targets against which recovery is measured. **They must not be represented as tested recovery capability** until a restore has been performed against them.

iii. The following recovery objectives apply:

Tier	Example Systems	Target RTO	Target RPO
Tier 1 — Critical	Core transaction processing, Ownest decisioning integration, POS partner integrations, payment/transaction data	4 hours weekdays / 12 hours weekends	24 hours
Tier 2 — Important	CRM/pipeline data, onboarding systems, internal productivity tools, internal communications	8 hours	24 hours
Tier 3 — Low	Marketing site, development environment, non-essential internal tools	48 hours	48 hours

a. *Incident Severity Levels and Activation Criteria*

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 notified within 30 minutes; full 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

Severity	Definition	Example	Activation
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

a. *Critical Services and Key Tasks*

i. The following are considered critical for business operations and must be restored in priority order:

1. Network and platform connectivity
2. CredX production backend services (Heroku Private Spaces, Canadian region)
3. The Ownest decisioning integration (UnderwriteFlow, Base44-hosted)
4. Payment and transaction data services
5. Merchant and partner support communication channels

ii. The following key tasks must be performed during a disaster recovery event, in accordance with CredX's objectives, agreements, and legal, contractual or regulatory obligations:

1. Determine the severity level per the table above and escalate accordingly.
2. Where a personal data breach is confirmed or suspected, begin the breach notification protocol in the Privacy Management Policy **immediately and in parallel** with technical recovery — do not wait for recovery to complete.
3. Notify affected merchants and regulated partners regarding the situation, actions taken, and recovery ETA when available. Where a partner is federally regulated, their OSFI reporting clock is 24 hours; CredX's notification must be fast enough not to become the bottleneck in that deadline.
4. Provide regular updates to affected merchants and partners with current status, actions taken, and a clear next-update time.
5. Restore systems and data prioritized by criticality tier, within the RTO and RPO targets above.

b. *Notification of Plan Initiation*

i. The following roles must be notified when this plan is initiated:

1. Incident Commander (Founder & CEO)
2. Technology & Infrastructure Lead (CTO)
3. Operations & Compliance Lead

ii. The Operations & Compliance Lead is responsible for notifying the personnel listed above, and for tracking regulatory notification obligations arising from the event.

c. *Plan Activation and Deactivation*

i. For P1 and P2 incidents, the Incident Commander is notified and formally activates this plan.

ii. This plan must only be deactivated by the Incident Commander (Founder & CEO) or, in their absence, the Technology & Infrastructure Lead (CTO).

iii. Before deactivation, the Technology & Infrastructure Lead must confirm that restored systems are functioning correctly and that data integrity has been verified. If CredX is still operating in an impaired scenario, the plan may be kept active at the discretion of the Incident Commander.

iv. The Incident Response Team must be notified when this plan is deactivated.

v. Within 5 business days of stand-down, the Incident Response Team documents root cause, timeline, response effectiveness, and corrective actions, and updates this policy and the risk register accordingly.

d. *Backup Requirements*

i. For each Tier 1 and Tier 2 system, CredX must document: backup frequency, retention period, storage location (geographically separate from production), encryption at rest and in transit, and the individual responsible.

ii. Minimum standards:

1. Daily automated backups of production data.
2. Encrypted backups retained for at least 90 days.
3. Backups tested via restore drill at least twice per year.

iii. Backups must respect the retention and deletion requirements of the Data Retention Policy and Privacy Management Policy. A deletion request that is honoured in production but not in backups is not honoured.

iv. Where contractually and technically permitted, CredX maintains its own export/backup of critical decisioning and merchant data **outside** the Ownest/Base44 environment, to avoid single-vendor lock-in risk.

v. **No restore drill has yet been performed against this policy** — confirming that backups are being taken is not the same as demonstrating a successful restore, and the twice-yearly drill requirement above remains outstanding.

e. *Vendor and Platform Dependencies*

i. CredX must obtain written backup, redundancy, and SLA documentation from Ownest for the Base44-hosted UnderwriteFlow decisioning environment, including backup frequency, restore process, and uptime history.

ii. CredX must establish a documented escalation contact and SLA with Ownest support for platform-level incidents.

iii. Because CredX licenses its core technology from Ownest Inc., which retains ownership, CredX must establish a technology continuity safeguard — source-code or technology escrow releasable on defined trigger events, a documented technical handover plan, or contractual continuity and support-SLA terms. **This risk is currently unmitigated.**

f. CredX must endeavor to restore its normal level of business operations as soon as possible.

g. *Pre-Authorized Actions*

i. During a crisis, certain recovery tasks must be performed immediately. The following are pre-authorized in the event of a disaster recovery event:

ii. The Technology & Infrastructure Lead must take all steps specified in this plan to recover CredX's information technology infrastructure and services.

iii. The Technology & Infrastructure Lead is authorized to make urgent purchases of equipment and services up to $10,000.

iv. The Technology & Infrastructure Lead is authorized to take immediate containment action before root cause is known — revoking compromised credentials, pausing affected integrations, isolating affected systems, and revoking tokens or disabling QR functionality.

v. The Operations & Compliance Lead is authorized to communicate with merchants and partners, subject to Incident Commander approval of the message content.

vi. The Operations & Compliance Lead is authorized to communicate with regulators and public authorities, including the Office of the Information and Privacy Commissioner of Alberta.

vii. The Technology & Infrastructure Lead is authorized to cooperate with Heroku, Ownest, POS integration partners (Clover, Square), and messaging providers (Twilio, SendGrid).

viii. **Only the Founder & CEO, or their explicit delegate, may speak publicly or to media about an incident.**

h. Specific recovery steps for information systems infrastructure and services are provided in Appendix B.

5 Appendix A: Relevant Points of Contact

5.1 Incident Response Team

Name	Mobile	Email
Kendall Raessler	403.200.9001	kendall@credxtech.com
Ray Yip	403.605.7012	ray@credxtech.com
Kyle Bunbury	403.464.9465	kyle@credxtech.com
Audrey Wilson	403.200.2244	audrey@credxtech.com

Incident roles are as listed in the Incident Response Team table above. **Audrey Wilson is the designated backup for all three other members; Ray Yip is Audrey Wilson's backup.**

All four addresses above are CredX addresses on a single mail domain. This is a deliberate change from the previously recorded personal and affiliate-company addresses, and it introduces a dependency worth stating plainly: **an incident affecting CredX's mail domain or Google Workspace tenancy degrades the primary contact path for the entire Incident Response Team at once.**

The **mobile numbers above are therefore the authoritative fallback**, and the phone/SMS tree — not email — is the contact method of record when Google Workspace is itself implicated in an incident. The Operations & Compliance Lead should maintain at least one out-of-band personal address per team member in the secure contact sheet held outside CredX systems, so that a mail-domain outage does not leave the team without a written channel.

This appendix must be kept current by the Operations & Compliance Lead, and a copy must be held **outside** systems that could themselves be affected by an incident — in particular, not solely in Google Drive, since Google Workspace is in scope.

Because each of CredX's four functions is currently staffed by one person, **functional unavailability is a named High risk**. Cover is provided by function, not by individual:

Function Unavailable	Covering Function
Leadership	Operations
Sales	Operations
Operations	Technical
Technical	Operations, with contracted technical support

The CEO confirms cover at the point of an incident. Operations can coordinate a Technical incident but cannot perform platform restoration, so a **pre-identified**

contract engineer is the real dependency for a Technical outage — retaining one in advance is a tracked action item.

5.2 External Contacts

External vendor and partner contacts, escalation paths, and SLA status are held in the Critical Vendor and Partner Register in the Business Continuity Plan. **No SLA is currently on file for any critical vendor**, and support and escalation contacts remain to be collected — a tracked action item owned by the Operations & Compliance Lead.

6 Appendix B: Recovery Steps for Information Systems Infrastructure & Services

Recovery is prioritized by criticality tier. Specific recovery procedures are described below.

Recovery Procedure	Person Responsible	Person(s) Notified When Complete
Tier 1 — Restore production services	CTO	Incident Commander
1. Confirm Heroku Private Spaces (Canadian region) availability and platform status	CTO	Incident Commander
2. Restore backend services and API	CTO	Incident Commander
3. Restore production data store to the most recent verified backup within RPO	CTO	Incident Commander
4. Confirm Ownest decisioning availability (UnderwriteFlow, Base44-hosted); escalate per vendor SLA	CTO	Incident Commander
5. Verify the decisioning path end to end — questionnaire, webhook, proposal request, loan terms	CTO	Incident Commander
6. Restore POS integrations, in order of merchant volume	CTO	Incident Commander
7. Verify token issuance, QR validation, and wallet delivery are functioning	CTO	Incident Commander
8. Confirm data integrity before declaring recovery complete	CTO	Incident Commander
Tier 2 — Restore internal operations	CTO / Operations	Incident Commander
1. Restore internal communication channels (Slack, Google Workspace)	Operations	Incident Commander
2. Restore Day.ai CRM access, or fall back to the most recent pipeline export	VP Sales / Operations	Incident Commander
3. Restore onboarding systems	Operations	Incident Commander
Tier 3 — Restore remaining services	CTO	Incident Commander
1. Restore marketing site and non-essential internal tools	CTO	Incident Commander
Staging and development environments	CTO	Incident Commander

Recovery Procedure	Person Responsible	Person(s) Notified When Complete
1. Restore staging environment after all production tiers are verified	CTO	Incident Commander

Recovery of environments must preserve environment isolation. Production data must not be restored into staging or development, and encryption keys must remain separated per environment.