Information Security Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Oct 31 2024	Updated roles and responsibilities

1 Purpose and Scope

1.1 Purpose

The purpose of this Information Security Policy is to ensure the confidentiality, integrity, and availability of CredX's information assets. This policy establishes a framework for managing information security risks and maintaining compliance with relevant security standards.

1.2 Scope

This policy applies to:

- All CredX employees, contractors, and third-party service providers.
- All information systems, networks, applications, databases, and assets used to process, store, or transmit CredX's information.
- Any information entrusted to CredX by customers, partners, and stakeholders.

2 Information Security Management

2.1 Governance & Compliance

- CredX shall establish an **Information Security Management System (ISMS)** to protect its assets and data.
- CredX's **Chief Information Security Officer (CISO)** is responsible for enforcing this policy.
- Compliance with **legal, regulatory, and contractual** obligations will be monitored regularly.

2.2 Risk Management

- CredX shall conduct **annual risk assessments** to identify threats, vulnerabilities, and their impact.
- A **risk register** shall be maintained to track identified risks and treatment plans.
- Security controls will be designed based on the **principle of least privilege (PoLP)** and **zero trust architecture**.

3 References

a. Encryption Policy

b. Data Center Security Policy
c. Disaster Recovery Policy
d. Password Policy
e. Remote Access Policy
f. Removable Media/Cloud Storage/BYOD Policy
g. Risk Assessment and Management Policy
h. Security Incident Response Policy
i. Software Development Lifecycle Policy
j. System Availability Policy
k. Workstation Security Policy

4 Roles & Responsibilities

4.1 Role Assignment

CredX does not maintain a standalone information security function. The security roles described in this policy are held by CredX's officers as follows:

- The **Chief Technology Officer (CTO)** holds the Chief Information Security Officer (CISO) and Information Security Manager (ISM) responsibilities described in this and all other CredX policies, and performs the operational duties attributed below to the IT Security Team.
- The **Founder & CEO** holds executive accountability for the information security program, including approval of policies, acceptance of residual risk, decisions on regulatory and law enforcement escalation, and reporting to any governing body. **CredX does not currently have a formal board of directors or independent oversight body**; establishing one as CredX scales is a tracked action item, and until then this program operates without independent internal challenge.

Where a policy requires ISM or CISO approval of an exception, risk acceptance, or expenditure, that approval is reserved to the Founder & CEO or the Leadership Team. Role assignment is recorded in the Organizational Narrative.

4.2 Chief Information Security Officer (CISO)

- Oversees the development and enforcement of security policies.
- Ensures compliance with regulatory and contractual obligations.
- Leads risk management and security incident response.
- Provides regular security reports to executive leadership.

4.3 IT Security Team

- Implements and maintains security controls and technologies.
- Monitors networks, systems, and logs for security incidents.
- Conducts vulnerability assessments and penetration testing.
- Manages access control mechanisms and enforces security policies.

4.4 Department Managers

- Ensure team compliance with security policies and procedures.
- Identify and mitigate security risks within their respective areas.
- Report security incidents and enforce access control measures.

4.5 Employees & Contractors

- Follow company security policies and guidelines.
- Complete required security awareness training.
- Report any suspicious activity or security incidents promptly.
- Secure company assets and protect sensitive information.

4.6 Third-Party Vendors

- Adhere to security requirements defined in contracts.
- Implement appropriate security measures to protect CredX's data.
- Report security breaches or incidents affecting CredX's systems.

5 Security Controls

5.1 Access Control

- Employees and third parties must be **authenticated and authorized** before accessing company assets.
- **Multi-factor authentication (MFA)** is required for all critical systems.
- **Periodic access reviews** shall be conducted to ensure proper user permissions.

5.2 Data Protection & Encryption

- **Encryption** must be applied to data **at rest** and **in transit** using industry-standard cryptographic algorithms.

- **Confidential data classification** shall be enforced with appropriate handling procedures.

5.3 Network & Infrastructure Security

- CredX will implement **firewalls, intrusion detection systems (IDS), and endpoint detection response (EDR)** solutions.
- Secure **network segmentation** will be enforced to limit access to critical environments.
- **Logging and monitoring** of system activity shall be maintained for security analysis.

5.4 Endpoint & Mobile Device Security

- All company-owned and BYOD devices must have **endpoint security software**.
- Devices must adhere to **Mobile Device Management (MDM)** policies.

5.5 Vendor & Third-Party Security

- CredX shall conduct **due diligence and security assessments** for vendors handling sensitive data.
- All third parties must sign **non-disclosure agreements (NDAs)** before accessing CredX's systems.

6 Security Awareness & Human Resources

6.1 Employee Training

- **Annual security awareness training** will be mandatory for all employees.
- Employees must undergo **security policy acknowledgment** during onboarding.

6.2 Secure Offboarding

- Access to systems shall be revoked immediately upon termination or role change.
- CredX IT must retrieve company-issued devices and ensure secure data disposal.

7 Incident Management

7.1 Security Incident Response

- CredX shall maintain an **Incident Response Plan (IRP)** for detecting, responding, and recovering from security incidents.
- Security events must be **reported within 24 hours** to the IT Security team.
- In the event of a **data breach**, affected customers must be notified per **legal and contractual requirements**.

8 Business Continuity & Disaster Recovery

- CredX shall maintain a **Business Continuity Plan (BCP)** and **Disaster Recovery Plan (DRP)** to ensure operations can continue after a security event.
- Backups shall be **encrypted, retained for at least 90 days, stored in a location geographically separate from production, and restore-tested at least twice per year**. **No restore test has yet been performed against this policy.**

9 Compliance & Enforcement

- CredX shall conduct **internal audits annually** to validate security controls.
- Non-compliance with this policy may result in **disciplinary action** or **termination of employment/contracts**.

This **Information Security Policy** will be reviewed and updated **annually** to reflect new security risks and regulatory changes.