Datacenter Policy

CredX Tech Inc

September 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.4

Table 2: Document history

Date	Comment
Sep 4 2026	Added AWS S3 ca-central-1 and at-rest encryption confirmation

1 Purpose and Scope

a. The purpose of this policy is to define security procedures within the organization's data centers and secure equipment areas.

b. This policy applies to any cloud hosted providers and facilities within the organization that are labeled as either a data center or a secure equipment area. Such facilities are explicitly called out within this document.

c. This policy applies to all management, employees and suppliers that conduct business operations within cloud host or data centers and secure equipment areas.

2 Background

a. This policy defines the policies and rules governing data centers and secure equipment areas from both a physical and logical security perspective. The document lists all data centers and secure equipment areas in use by the organization, prescribes how access is controlled and enforced, and establishes procedures for any visitor or third party access. This policy also defines prohibited activities and requirements for periodic safety and security checks.

3 Policy

a. The following locations are classified by the organization as secure areas and are governed by this policy:

   i. **Heroku Private Spaces, Canadian region** — backend service, database, and cache hosting for the production environment. **All PII and payment-related workloads are confined to the Canadian Private Space** to meet data residency requirements.

   ii. **AWS S3, `ca-central-1` (Canada Central)** — object storage for merchant logo images only. No PII or transaction data. Server-side encryption applies via the bucket default; the application does not request it explicitly.

   iii. **Ownest / Base44 decisioning environment** — hosts the UnderwriteFlow credit questionnaire and decisioning application operated by affiliated company Ownest Inc. **This environment is outside CredX's system boundary**; provider region, backup, and redundancy architecture are not yet documented. **[TBD]**

   iv. **CredX corporate premises — Suite 159 #406, 917-85 St SW, Calgary, AB T3H 5Z9.** No production infrastructure is hosted at this location. Physical access is governed by the Office Security Policy.

b. CredX operates no on-premises data centers. All production infrastructure is hosted in cloud provider facilities. Physical and environmental controls at those facilities are the responsibility of the provider, and are verified through Tier 1 vendor due diligence under the Vendor Management Policy, including review of a current SOC 2 Type II report or equivalent third-party certification at onboarding and annually thereafter.

c. **Data residency.** PII and sensitive customer data must be processed and stored within Canada-based infrastructure. Both CredX-controlled stores meet this: the application and PostgreSQL database run in Heroku Private Spaces (Canadian region), and object storage is AWS S3 in `ca-central-1`, configured identically across development, staging, and production. Cross-border data transfers must be explicitly reviewed, documented, and approved before they occur.

d. **Encryption at rest.** Both stores encrypt data at rest at the platform layer — Heroku Postgres with platform-managed AES-256, S3 with server-side encryption. Note that platform-layer encryption does not substitute for the application-layer field encryption required by the Encryption Policy, which is not implemented.

e. **Environment isolation.** Development, staging, and production environments must be isolated using separate Private Spaces or strict network segmentation. Encryption keys must be separated per environment, and production data must not be restored into a non-production environment.

f. **Network restriction.** Inbound traffic must be restricted using IP allowlists, private networking, and internal routing where possible. All access is HTTPS-only.

g. **Known gap.** Backup and replication architecture within Heroku Private Spaces is not finalized, multi-region and failover redundancy is not confirmed, and no SOC 2 report or equivalent has yet been obtained from Ownest. This policy states required practice; it is not evidence that these controls are verified.

h. The visitor access, physical marking, and prohibited activity requirements below apply to on-premises secure equipment areas under CredX's direct control. Where CredX holds no physical control, the equivalent provider controls evidenced under vendor due diligence apply in their place.

i. Each data center and secure area must have a manager assigned. The manager's name must be documented in the organization's records. In the case of any on-prem data centers, the manager's name must also be posted in and near the secure area.

j. Each secure area must be clearly marked. Access to the secure area must be controlled by at least a locked door. A visitor access log must be clearly marked and easily accessible just inside the door.

k. Persons who are not employed by the organization are considered to be visitors. Visitors accessing secure areas shall:
    i. Obtain access to secure areas in accordance with reference a.
    ii. Only enter and remain in secure areas when escorted by a designated employee. The employee must stay with the visitor during their entire stay inside the secure area.
    iii. Log the precise time of entry and exit in the visitor access log.
l. The following activities are prohibited inside secure areas:
    i. Photography, or video or audio recordings of any kind.
    ii. Connection of any electrical device to a power supply, unless specifically authorized by the responsible person.
    iii. Unauthorized usage of or tampering with any installed equipment.
    iv. Connection of any device to the network, unless specifically authorized by the responsible person.
    v. Storage or archival of large amounts of paper materials.
    vi. Storage of flammable materials or equipment.
    vii. Use of portable heating devices.
    viii. Smoking, eating, or drinking.
m. Secure areas must be checked for compliance with security and safety requirements on at least a quarterly basis.