Data Retention Policy

CredX Tech Inc

September 2026

Contents

1 Appendices **2**

2 Purpose and Scope **2**

3 Background **2**

4 Policy **3**

5 Appendix A: Retention Periods **6**

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.2, CC6.5, P4.2

1 Appendices

Appendix A: Retention Periods

2 Purpose and Scope

a. This data retention policy defines the objectives and requirements for data retention within CredX Tech Inc.

b. This policy covers all data within CredX Tech Inc's custody or control, regardless of the medium the data is stored in (electronic form, paper form, etc.) Within this policy, the medium which holds data is referred to as information, no matter what form it is in.

c. This policy applies to all users of information systems within CredX Tech Inc. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information CredX Tech Inc owns or controls (hereinafter referred to as "users"). This policy must be made readily available to all users.

3 Background

a. CredX Tech Inc is bound by multiple legal, regulatory and contractual obligations with regard to the data it retains. These obligations stipulate how long data can be retained, and how data must be destroyed. Examples of legal, regulatory and contractual obligations include laws and regulations in the local jurisdiction where CredX Tech Inc conducts business, and contracts made with employees, customers, service providers, partners and others.

b. CredX Tech Inc may also be involved in events such as litigation or disaster recovery scenarios that require it to have access to original information in order to protect CredX Tech Inc's interests or those of its employees, customers, service providers, partners and others. As a result, CredX Tech Inc may need to archive and store information for longer that it may be needed for day-to-day operations.

4 Policy

a. *Information Retention*

   i. Retention is defined as the maintenance of information in a production or live environment which can be accessed by an authorized user in the ordinary course of business.

   ii. Information used in the development, staging, and testing of systems shall not be retained beyond their active use period nor copied into production or live environments.

   iii. By default, the retention period of information shall be an active use period of exactly two years from its creation unless an exception is obtained permitting a longer or shorter retention period. The business unit responsible for the information must request the exception.

   iv. After the active use period of information is over in accordance with this policy and approved exceptions, information must be archived for a defined period. Once the defined archive period is over, the information must be destroyed.

   v. Each business unit is responsible for the information it creates, uses, stores, processes and destroys, according to the requirements of this policy. The responsible business unit is considered to be the information owner.

   vi. CredX Tech Inc's legal counsel may issue a litigation hold to request that information relating to potential or actual litigation, arbitration or other claims, demands, disputes or regulatory action be retained in accordance with instructions from the legal counsel.

   vii. Each employee and contractor affiliated with the company must return information in their possession or control to CredX Tech Inc upon separation and/or retirement.

   viii. Information owners must enforce the retention, archiving and destruction of information, and communicate these periods to relevant parties.

b. *Information Archiving*

   i. Archiving is defined as secured storage of information such that the information is rendered inaccessible by authorized users in the ordinary course of business but can be retrieved by an administrator designated by company management.

      1. Physical (e.g., paper) records must be archived in secured storage (onsite or offsite) and clearly labeled in archive boxes naming the information owner.

2. Electronic records must be archived with strict access controls set by the information owner and appropriate to secure the confidentiality, integrity and accessibility of the information.

ii. The default archiving period of information shall be 7 years unless an approved exception permits a longer or shorter period. Exceptions must be requested by the information owner.

1. As a guideline, an archiving period of more than 7 years may be granted for information with a vital historical purpose such as corporate records, contracts, and technical/trade secrets.

2. As a guideline, an archiving period of less than 7 years may be granted for information with a limited business purpose such as email, travel itineraries, pre-trip advisories, or to comply with specific legal, contractual and/or regulatory requirements (e.g., PCI DSS, GDPR, etc.)

iii. Information must be destroyed (defined below) at the end of the elapsed archiving period.

c. *Information Destruction*

i. Destruction is defined as the physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially-available means.

ii. CredX Tech Inc must maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived, whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files. Physical information in paper form must be shredded using an authorized shredding device; waste must be periodically removed by approved personnel.

d. Retention and archival periods for information that is created, processed, stored and used by CredX Tech Inc is defined in Appendix A, "Retention Periods."

Retention Requirements Specific to Regulated Data

e. **Retention policies must be defined per PII category**, with automated purge when data is no longer required. *This has not yet been formalized — completing it is a tracked action item.*

f. **Backups must respect retention and deletion policies.** A deletion request honoured in production but not in backups is not honoured.

g. **User-initiated deletion requests must be supported**, per the Privacy Management Policy.

h. **A record of every breach of security safeguards must be kept for at least 24 months** and produced to the regulator on request, regardless of whether a real risk of significant harm was determined and regardless of whether notification was required. This is a statutory obligation under both Alberta PIPA and PIPEDA.

i. **Credit bureau data retention is bounded by the licensed lender's permissible purpose** and the terms of the bureau and lender agreements, not solely by CredX's own schedule.

j. **Automated decision records** — the model version, inputs, outcome, and any human review — must be retained for the period stated below so that an adverse decision can be substantiated to the applicant, the lending partner, and a regulator.

5 Appendix A: Retention Periods

Information Type	Information Owner	Storage Location	Retention Period	Archival Period
User and merchant account records	CTO	Heroku Private Spaces (CA)	Active account + 2 years	7 years
Applicant PII (onboarding, KYC support, digital ID results)	Operations	Heroku Private Spaces (CA)	**[TBD — per PII | Per lender | category; not yet | agreement | formalized]**	
Loan proposals and decisioning and underwriting outputs	CTO	Ownest (Base44-hosted)	Per licensed lender's permissible purpose and agreement	Per lender agreement **[TBD]**
Automated decision records (model version, inputs, outcome, human review)	CTO	Heroku Private Spaces (CA)	7 years	7 years
Consent records and consent revocation history	Operations	Heroku Private Spaces (CA)	Life of relationship + 7 years	7 years
Transaction and payment records	Founder & CEO	Heroku Private Spaces (CA)	7 years	7 years
POS integration transaction metadata	CTO	Heroku Private Spaces (CA)	Per POS partner agreement **[TBD]**	Per partner agreement
Value-back balances and redemption records	Operations	Heroku Private Spaces (CA)	Active account + 2 years	7 years
Merchant Network Agreements and partner contracts	Founder & CEO	Corporate records	Contract term + 7 years	7 years
CRM pipeline records	VP Sales	Day.ai	2 years	None

Information Type	Information Owner	Storage Location	Retention Period	Archival Period
PII access, authentication, QR validation, and payment logs	CTO	Heroku Private Spaces (CA)	12 months	7 years
Breach record log (all breaches of security safeguards, regardless of RROSH)	Operations	Corporate records	**24 months minimum** (PIPA/PIPEDA statutory)	7 years
Database backups	CTO	**[TBD — architecture not finalized]**	**90 days minimum (recommended)**	None
Compliance and policy records	CTO	Source control	7 years	7 years
Security incident records	CTO	JIRA	7 years	7 years
Access and vendor review records	CTO	JIRA	7 years	7 years
Training completion records	Founder & CEO	Policy Training Ledger	7 years	7 years
Vendor contracts and DPAs	Founder & CEO	Corporate records	Contract term + 7 years	7 years
Employee and contractor records	Founder & CEO	Corporate records	Engagement + 7 years	7 years