POLICY

Data Retention & Disposal Policy

Zencode Consulting Inc. retains personal, confidential, and other sensitive information only for as long as it is reasonably required, and disposes of it when it is no longer needed.

ORGANIZATION
Zencode Consulting Inc.

DOCUMENT
Data Retention & Disposal Policy

VERSION
1.0

EFFECTIVE
August 14, 2026

POLICY OWNER
Owner / Information Security Lead

REVIEW FREQUENCY
At least annually and following material changes

LAST REVIEWED
August 14, 2026

1. Purpose

Zencode Consulting Inc. maintains this policy to ensure that personal, confidential, and other sensitive information is retained only for as long as it is reasonably required and is securely disposed of when no longer needed.

The objectives of this policy are to:

- minimize unnecessary retention of sensitive information
- define consistent retention practices
- support applicable privacy, security, contractual, and legal obligations

- reduce the consequences of unauthorized access
- provide procedures for deletion and secure disposal
- ensure retention practices are periodically reviewed

2. Scope

This policy applies to information processed or controlled by Zencode in connection with:

- Zencode-operated applications
- customer and consumer services
- production infrastructure
- financial-data integrations
- administrative systems
- operational and security records
- backups
- development and support activities

The policy applies regardless of whether information is stored directly by Zencode or by a service provider acting on Zencode's behalf.

3. Retention principles

Zencode follows these principles:

Purpose limitation. Information should be retained only while it serves a documented business, service, security, contractual, or legal purpose.

Data minimization. Systems should avoid collecting or retaining information that is not required.

Defined retention. Categories of sensitive information should have an identified retention rule or disposal trigger.

Secure disposal. Information that is no longer required should be securely deleted, destroyed, anonymized, or rendered inaccessible as appropriate to the storage medium.

Legal requirements take precedence. Where applicable law, litigation requirements, contractual obligations, fraud prevention, or another legitimate requirement mandates longer retention, that requirement supersedes the normal schedule.

4. Financial consumer data

Applications that access consumer financial information must minimize the information they retain.

For read-only financial-data integrations:

- raw API responses should not be persistently retained unless required for the operation of the service
- provider access credentials must be encrypted and retained only while the associated connection remains active
- detailed financial information should be reduced to the minimum information required by the application
- transaction history should not be collected where the application does not require it
- provider credentials and financial information must not be intentionally written to application logs

When a consumer revokes or removes a financial connection, associated financial information should be removed from active systems unless continued retention remains required for a lawful and documented purpose.

5. Standard retention schedule

Unless a more specific legal or contractual requirement applies, Zencode uses the following baseline schedule.

Active account information

Retained while the user or customer account remains active and the information is required to provide the service.

Following account deletion, information no longer required is removed from active production systems as soon as reasonably practicable and ordinarily within **7 days**.

External financial connection credentials

Retained only while the user maintains the applicable connection.

On disconnect or account deletion:

- provider access is revoked where supported
- stored connection credentials are deleted from active systems

Raw financial-provider responses

Not persistently retained as a normal operating practice.

Responses may be processed transiently to obtain the values required by the service and then discarded.

Current financial values

Retained only while required to provide the requested service.

Source-specific values are deleted when the associated source is removed unless a documented exception applies.

Public financial-verification records

Public verification records should have a defined expiry period.

For LOADED, the initial default maximum retention for independently addressable verification snapshots should be **30 days**, unless the user deletes or invalidates the verification sooner.

When the contributing financial authorization is revoked, a public verification depending on that information should be invalidated.

Application logs

General production application logs are normally retained for no more than **30 days**.

Application logs must be designed not to contain:

- provider access tokens
- passwords
- financial account credentials
- raw financial-provider responses
- individual financial balances except where strictly required for investigating a specific incident

Security and audit records

Security and administrative audit records may be retained for up to **90 days**, or longer where reasonably required for investigation, fraud prevention, security response, or legal obligations.

Sensitive financial payloads should not be included in ordinary security logs.

Consent and privacy-request records

Records necessary to document consent, account-deletion requests, privacy requests, or compliance actions may be retained for as long as reasonably necessary to demonstrate and administer those obligations.

These records should contain the minimum personal information required for that purpose.

Encrypted backups

Production backups containing deleted information may continue to contain that information temporarily until the backup expires.

Normal backup retention should not exceed **30 days** unless a documented operational, contractual, or legal requirement requires a longer period.

Deleted information must not be intentionally restored into active service except as part of a legitimate disaster-recovery event.

If a backup containing previously deleted information is restored, applicable deletion actions must be reapplied.

Accounting, tax, contractual, and legal records

Records required for taxation, accounting, contractual, litigation, regulatory, or other legal purposes may be retained for the period required by applicable law or legitimate business obligations.

Financial-account data obtained solely to operate a consumer application should not be retained merely because unrelated corporate accounting records must be preserved.

6. Disposal procedures

Electronic records

When electronic information reaches the end of its retention period or a deletion trigger occurs, Zencode:

- deletes the records from active production systems using the storage platform's ordinary deletion controls
- revokes associated provider access tokens where the provider supports revocation
- invalidates public or shared records that depend on the deleted information
- destroys or discards encryption keys or access tokens that would otherwise leave residual ciphertext usable, where that is the applicable control

Deleted electronic records may remain in encrypted backups until those backups expire under the backup schedule.

Zencode does not rely on informal “delete the file later” handling for production consumer or financial records. Deletion is performed through the application's account-deletion and connection-removal paths, or through equivalent administrative action.

Physical media

Zencode does not use removable physical media as a normal store for consumer financial information.

If physical media containing sensitive information is used, it is securely wiped or physically destroyed before reuse or disposal. Paper copies, if created, are shredded or otherwise destroyed so the information cannot be reconstructed in ordinary use.

Third-party processors

Where a service provider stores information on Zencode's behalf, disposal is performed using that provider's deletion, revocation, or retention controls.

Provider-side backups may retain deleted information until those backups expire. Zencode does not treat a provider backup lag as permission to restore deleted consumer financial information into active service except for legitimate disaster recovery, after which applicable deletion actions must be reapplied.

7. Exceptions

An exception is a documented deviation from this policy.

- Exceptions are approved by the Owner / Information Security Lead.
- Each exception records the information category, the reason, any compensating control, the expiry or review date, and who is affected.
- Exceptions are reviewed at least annually and closed when no longer needed.
- An exception does not authorize indefinite retention of consumer financial information, sale of financial information, or restoration of deleted consumer data except for legitimate disaster recovery.

8. Roles and review

The Owner / Information Security Lead owns this policy, approves exceptions, and is responsible for the periodic review.

Personnel who operate Zencode systems are responsible for following the retention schedule and for using the application's deletion and revocation paths rather than retaining copies outside those systems.

This policy is reviewed at least annually and following material changes to systems, data handling, or legal requirements. The **Last reviewed** date is updated when the review is completed.

Related public summary: Security & Data Protection.

9. Contact

Questions about this policy: security@zencode.ca.

A PDF copy is available at zencode.ca/data-retention/zencode-consulting-inc-data-retention-disposal-policy.pdf.