Data Deletion Policy

1. Overview

At Miigwech AI Solutions, we respect your right to control your information. miigEngine is designed for sovereign, on-premises deployment on your infrastructure, giving you complete control over all AI inference activity, session data, and any associated logs. This policy explains:

- What data miigEngine typically stores locally.
- Where deletion and retention are controlled by you vs. Miigwech.
- Recommended patterns for secure deletion and retention.

miigEngine does not transmit operational data to Miigwech. In virtually all cases, you are the sole party with the ability to access, retain, or delete data generated by your miigEngine deployment.

2. Data Categories in miigEngine

In a standard deployment, miigEngine may handle:

- Identity and access data — User accounts, roles, password hashes, session tokens, API keys.
- Inference session data — Prompts submitted by users, model outputs, conversation history (where session persistence is enabled).
- Uploaded documents — Files submitted to the AI for processing or retrieval-augmented inference.
- Operational logs — HTTP/audit logs for the admin UI and APIs, system events, login events.
- Ephemeral data — Short-lived session cookies, cache, and transient inference state.

Exact data categories depend on how you configure and use your miigEngine instance.

3. Who Controls Deletion

Because miigEngine is deployed on your infrastructure:

- You control the storage systems (disks, databases, session stores, backups) where miigEngine data resides.
- You control when data is deleted, anonymized, or retained under your own policies.
- Miigwech does not reach into your environment to delete or retain any data unless explicitly agreed in a managed-service contract.

If Miigwech also operates a hosted miigEngine instance on your behalf, that hosted environment will have a separate, written data retention/deletion schedule as part of your service agreement.

4. Deletion Mechanisms (Typical Patterns)

4.1 User Accounts and Access

Administrators can disable or remove accounts using the miigEngine admin interface or API. Typical effects:

- Disable user — prevents login; account record and historical logs remain.
- Delete user (where implemented) — removes the user record; logs may retain a non-identifying reference (e.g., a numeric ID) for audit integrity.

We recommend:

- Deactivate users for most HR/lifecycle events.
- Use anonymization or log rotation (see 4.3) if you need to remove identifying information from historical logs.

4.2 Inference Session Data and Uploaded Documents

Deletion of session history and uploaded documents is fully under your control:

- Use your database tools, admin interface, or application logic to delete session records, conversation histories, and uploaded files.
- miigEngine does not silently mirror or back up your inference data to Miigwech-controlled infrastructure.
- If you implement operational scripts or CLI tools for bulk deletion, document them in your internal runbooks rather than relying on them as hardwired guarantees from Miigwech.

4.3 Audit Logs and System Logs

By default, miigEngine can record audit logs (e.g., timestamp, method, path, status, remote IP, user ID) for security and compliance purposes. Recommended pattern:

- Short-term detailed logs (e.g., 30–90 days) for active investigations and incident response.
- Optional longer-term, reduced logs (e.g., summarized or anonymized) if you need historical metrics without personal identifiers.

Implement log rotation and deletion via:

- Database retention jobs (e.g., scheduled DELETE FROM audit_logs WHERE timestamp < ...).
- Filesystem rotation for any text-based logs (e.g., logrotate).

miigEngine does not force a retention schedule; you define this based on your legal and policy obligations.

5. Ephemeral Session and Inference Data

By default, miigEngine handles inference transiently:

- In-flight prompts and outputs are processed in memory and not persisted to long-term storage unless your configuration explicitly enables session history.
- Session cookies are short-lived, http-only, and local to the user's browser session. They are not stored server-side beyond the active session.
- Conversation exports downloaded by users are delivered directly to the user's device and are not retained by miigEngine after delivery.

These behaviors are part of miigEngine's privacy-by-default design and are intended to minimize persistence of sensitive inference content.

6. Backups, Snapshots, and Emergency Deletion

Because miigEngine runs inside your environment:

- Backups and snapshots (e.g., database dumps, volume snapshots) are created, stored, and deleted according to your own policies.
- If you restore from an older backup, previously deleted session data or documents may reappear until deleted again.

For emergency deletion (e.g., credential compromise, incident response), your administrators can:

- Revoke user credentials and session tokens.
- Delete specific session histories, conversation records, or uploaded document stores.

- Purge or rotate logs.
- Destroy or overwrite storage volumes.

Miigwech can provide guidance or scripts as part of support, but actual deletion is performed by your team unless a managed-service contract states otherwise.

7. Irreversibility and Recovery

miigEngine is intentionally designed so that:

- Miigwech does not maintain shadow copies of your inference data, prompts, outputs, or documents outside of your control.
- If your team deletes data from your environment (and from any backups and snapshots you control), Miigwech cannot restore it for you.
- You are responsible for implementing and testing a backup and recovery strategy consistent with your own retention obligations and risk tolerance.

8. Alignment with Sovereignty and Privacy Frameworks

This approach to data retention and deletion is intended to support:

- OCAP® principles (Ownership, Control, Access, Possession) for First Nations data governance.
- PIPEDA and applicable Canadian privacy laws regarding limiting collection, retention, and use.
- Data sovereignty expectations where communities and public bodies require that AI inference data remain in their legal and physical control.
- The spirit of the "right to erasure" under GDPR-like frameworks, to the extent you implement deletion and anonymization workflows in your environment.

9. How to Exercise Deletion or Retention Choices

Because miigEngine is deployed in your environment:

- End-users should send access or erasure requests to your organization, not to Miigwech.
- Your administrators can then:
- Disable or delete accounts in miigEngine.
- Delete or anonymize conversation histories, session records, and uploaded documents.
- Apply log retention and deletion policies per your governance framework.

If you operate a Miigwech-hosted instance, details of how we execute deletion on your behalf (and timelines) will be documented in your service agreement and/or Data Processing Addendum.