Data Access & Visibility Overview

Document ID: DP-ACCESS-001
Version: 1.0
Effective Date: February 2026
Classification: Public

---

1. Purpose

This document provides a concise public summary of Clarity AI Lab's data access architecture and visibility controls across its AI-powered systems, including:

- Maimai Supply
- Studio Clarté

This overview supports transparency for enterprise customers, institutional partners, and regulators.

---

2. Architectural Access Model

Clarity AI Lab operates a restricted-visibility system architecture designed to minimize internal access to customer-generated content.

2.1 No Routine Administrative Visibility

- Administrative dashboards are limited to account-level management functions (e.g., account deletion, subscription status, credential reset).
- Administrative interfaces do not provide browsing or inspection capability for customer workspace content.
- Internal personnel do not have routine dashboard-based visibility into customer-generated data.

AI-generated outputs remain under user control and are not independently reviewed by Clarity AI Lab in the ordinary course of operations.

---

3. Logging & Monitoring Controls

Clarity AI Lab utilizes cloud-based monitoring tools to maintain system integrity and operational reliability.

3.1 No Content Logging

Monitoring systems are configured to avoid capturing or retaining:

- Customer prompts
- Workspace documents
- AI-generated drafts
- Structured user content

Logs are limited to operational metadata necessary for:

- Authentication validation
- Infrastructure health monitoring
- Security event detection
- Service performance measurement

---

4. Debugging & Development Practices

Production debugging does not rely on live customer content.

- Testing and quality assurance processes use synthetic, anonymized, or controlled test datasets.
- Where content-level investigation is required for support purposes, customers must voluntarily provide specific information for review.
- Production and non-production environments are logically separated.

---

5. Role-Based Access Controls

Access to infrastructure is governed by:

- Role-Based Access Control (RBAC)
- Least-privilege principles
- Multi-factor authentication for privileged roles
- Logged administrative actions
- Annual access review procedures

Administrative roles do not include content-browsing capability through production dashboards.

Any exceptional access required for incident response or legal compliance is subject to documented authorization and logging in accordance with SEC-001 (Incident Response & Breach Notification Plan).

---

6. Metadata vs. Content Distinction

For clarity:

- **Customer Content** refers to user-generated prompts, documents, drafts, or structured workspace materials.
- **Operational Metadata** refers to limited system-level data such as account identifiers, authentication events, usage timestamps, and infrastructure alerts.

This document's access limitations apply to customer content.
Operational metadata may be processed as necessary for security, reliability, and compliance purposes.

---

7. Vendor & Regional Processing Controls

Clarity AI Lab utilizes third-party cloud and AI infrastructure providers, including:

- Google Cloud
- Google Gemini APIs

Where available, regional processing configurations are used to align with customer residency requirements.

Vendor contracts are reviewed periodically to confirm:

- Data handling commitments
- Non-training use of customer inputs (where contractually specified)
- Security and confidentiality safeguards

Clarity AI Lab does not independently train foundation models using customer-generated content.

---

8. Human Oversight & User Control

All AI outputs are advisory in nature.

Users retain full authority to:

- Accept
- Reject
- Modify
- Independently verify

AI-generated outputs prior to operational reliance.

Clarity AI Lab systems are not designed for autonomous consequential decision-making.

---

9. Continuous Review

This Data Access & Visibility Overview is reviewed annually and updated following material architectural or regulatory changes.

For governance documentation, see:

- GOV-001 — AI Governance Charter
- DP-001 — Master Privacy Policy
- ARCH-002 — Restricted Architecture & Security Controls Supplement
- SEC-001 — Incident Response & Breach Notification Plan

End of DP-ACCESS-001