Access Rights Review Policy

Synthetic Users

Version: 1.2

Effective Date: January 2024

Last Updated: March 25, 2026

Document Owner: CTO — Artur Ventura

Review Frequency: Annually

Classification: Internal – Confidential

CRA Reference: 9.1.1

Change History

Version	Date	Author	Changes
1.1	January 2024	CTO / Security Lead	Initial release
1.2	March 25, 2026	Artur Ventura, CTO	Added version metadata and last review date; expanded system scope to include AI/GenAI infrastructure; added Section 11 (AI/GenAI System Access Controls) covering LLM provider credentials, RAG pipeline access, Persona Engine, and privileged AI system roles; added related documents. Per JPMC SCA CRA 9.1.1.

---

1. Purpose

To ensure that all user access to Synthetic Users company systems, applications, and data is appropriate and aligns with current job responsibilities, thereby enhancing security and minimizing unauthorized access risks.

2. Scope

This policy applies to all employees, contractors, and third-party users who have access to the company's information systems, including but not limited to:

- Cloud infrastructure (AWS, Render)
- Source control and CI/CD (GitHub, deployment pipelines)
- Productivity and internal tools (Notion, Intercom, Google Workspace)
- AI/GenAI infrastructure (LLM provider API credentials, RAG pipeline, Persona Engine, LLM Shuffle configuration)
- Data stores (databases, vector stores, object storage)
- Security tooling (monitoring, logging, alerting platforms)

3. Responsibilities

Management / CTO: Oversees implementation of this policy, approves high-risk access changes, and ensures compliance.

IT Administrator (or Assigned Personnel): Executes the access rights review process, maintains records, and implements access changes.

Employees: Use access privileges responsibly, operate on a least-privilege basis, and report any access discrepancies immediately.

4. Authentication and Access Controls

- All system access requires Single Sign-On (SSO) with Multi-Factor Authentication (MFA).
- Permissions are managed using Role-Based Access Control (RBAC) to ensure users only have access to the resources necessary for their role.
- Default access is limited to the minimum necessary privilege.
- Privileged and administrative access is separated from day-to-day user accounts.

5. Access Rights Review Process

Frequency: Access rights are reviewed semi-annually (twice a year) or whenever there is a significant change in staff roles, system architecture, or third-party relationships.

Process Steps:

a. Listing Access Rights — Compile a complete list of all users and their current access rights across all in-scope systems and data.

b. Review — Management reviews the list to confirm that access levels are appropriate for each user's role. AI/GenAI system credentials and privileged accounts receive specific review attention (see Section 11).

c. Adjustment — Modify or revoke access rights that are no longer necessary, including stale credentials, overly broad permissions, and access retained after role changes.

d. Documentation — Record all changes made, including the date and reason for each adjustment. Records are retained for a minimum of 12 months.

6. Onboarding and Offboarding

New Employees: Access rights are granted based on job requirements upon joining. Access follows the least-privilege principle — additional access is requested and approved through the standard change process.

Departing Employees: All access rights are revoked immediately upon termination or resignation, including SSO accounts, cloud credentials, AI/GenAI API keys, and any personal tokens or service credentials provisioned to the individual.

7. Role Changes

Access rights are reviewed and adjusted whenever an employee changes roles to ensure they have necessary and appropriate access only. Prior role access is revoked before or at the time of transition.

8. Temporary Access

Temporary access requires management approval and must be set with a defined expiration date. Temporary access is documented and reviewed at the next scheduled review cycle to confirm it was revoked as planned.

9. Reporting and Compliance

- Employees must report any unauthorized access or suspected security breaches immediately via the incident reporting process.
- Non-compliance with this policy may result in disciplinary action.
- Access review records are retained for a minimum of **12 months** for audit purposes.

10. Review and Update of the Policy

This policy is reviewed annually and updated as needed to reflect changes in systems, personnel, and regulatory requirements. Access review logs and documentation are retained for a minimum of 12 months.

11. AI/GenAI System Access Controls

AI/GenAI systems at Synthetic Users (LLM provider APIs, RAG pipeline, Persona Engine, LLM Shuffle) involve sensitive credentials and privileged configuration access. These systems are subject to all standard access controls in this policy, with the additional requirements below.

11.1 LLM Provider API Credentials

- API keys for LLM providers (OpenAI, Anthropic, Google, and others) are treated as privileged credentials.
- Keys are stored in a secrets manager and are not embedded in source code or configuration files.
- Access to retrieve or rotate LLM API keys is restricted to the CTO and authorized engineering personnel.
- Keys are rotated at least annually or immediately upon any suspected compromise or personnel departure.

11.2 RAG Pipeline and Vector Store Access

- Access to the RAG pipeline (retrieval indexes, vector stores, embedding pipelines) is restricted to authorized AI/ML engineering roles.
- Tenant data isolation is enforced at the storage layer — no cross-tenant retrieval access is permitted.

- Privileged access to the vector store (bulk read, delete, or reindex operations) requires CTO approval.

11.3 Persona Engine and LLM Shuffle Configuration

- System prompt configuration in the Persona Engine is treated as a privileged asset.
- Changes to system prompts or LLM Shuffle routing rules require CTO sign-off per the Change Management Policy.
- Access to make configuration changes is restricted to authorized personnel only.

11.4 AI/GenAI Access Review Cadence

AI/GenAI system credentials and access roles are explicitly included in the semi-annual access rights review (Section 5). The review confirms:

Access Type	Review Action
LLM provider API keys	Confirm active keys are in use; rotate any stale or unused keys
RAG pipeline access	Confirm role assignments match current engineering team
Persona Engine config access	Confirm only authorized personnel retain write access
LLM Shuffle routing config	Confirm only authorized personnel retain write access
Vector store privileged access	Confirm no stale privileged grants exist

---

12. Related Documents

- Password Management Policy — Credential strength, rotation, and lockout requirements
- Change Management Policy — Approval process for AI/GenAI configuration changes
- Third-Party Risk Management Policy — LLM provider access and DPA status

- Incident Response Plan — Unauthorized access incident procedures
- Information Governance & Records Management Standard — Access log retention requirements