Synthetic Users Records & Document Management Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines how Synthetic Users manages, stores, and controls organizational records and documents throughout their lifecycle, ensuring accessibility, integrity, and compliance with retention requirements.

2. Scope

This policy applies to all corporate records, policies, procedures, and documentation maintained by Synthetic Users, including both physical and logical records. As a fully digital organization, Synthetic Users does not maintain physical records.

3. Document Management Systems

Synthetic Users uses two primary systems for document and records management:

3.1 Legal & Compliance Documentation — Git-Backed Website

- All policies, procedures, compliance documentation, and legal documents are maintained on the legal documentation site (legal.syntheticusers.com).
- The site is backed by **Git**, providing:
  - Full version history and audit trail for every document change
  - Peer review via pull requests before publication
  - Immutable commit history ensuring document integrity
  - Attribution of all changes to specific authors with timestamps
- This serves as the **system of record** for all compliance and legal documentation.

3.2 Operational Documentation — Notion

- Internal operational documentation, project records, meeting notes, and working documents are maintained in **Notion**.
- Notion provides access controls, version history, and search capabilities for internal documentation.

---

4. Records Lifecycle

4.1 Creation

- All records are created in the appropriate system (Git-backed site for policies, Notion for operational documents).
- Records must be clearly titled, dated, and attributed to an owner.

4.2 Classification

Records are classified as:

Classification	Description	Examples

Policy	Approved governance documents	Security policies, compliance documentation
Procedure	Operational processes	Incident response procedures, onboarding checklists
Evidence	Audit and compliance artifacts	SOC 2 reports, penetration test results, training records
Operational	Internal working documents	Meeting notes, project plans, design documents

4.3 Storage & Access

- Policy and compliance records are stored in the Git repository with access restricted to authorized personnel.
- Published documentation is available at legal.syntheticusers.com for customer and auditor access.
- Operational records in Notion are access-controlled by workspace and team permissions.

4.4 Retention

- Policy documents are retained indefinitely with full version history in Git.
- Compliance evidence (SOC 2 reports, penetration tests) is retained for a minimum of 3 years.
- Operational records are retained per the Data Deletion and Retention Policy.

4.5 Disposal

- Records past their retention period are reviewed before disposal.
- Disposal of compliance records requires approval from the Security & Compliance Lead.
- Deleted records from Git are retained in Git history and can be recovered if needed.

---

5. Information Governance

- All policy documents are reviewed and updated at least annually.
- Document owners are responsible for ensuring their records are current and accurate.
- The Security & Compliance Lead maintains an index of all active policies and their review dates.

6. Review

This policy is reviewed annually or when changes to document management systems occur.