Synthetic Users Information Governance & Records Management Standard

Document ID: CRA-34.1.1-IGRMS-001

Version: 1.0

Effective Date: March 25, 2026

Last Updated: March 25, 2026

Owner: CTO — Artur Ventura

Approved By: CEO — Kwame Ferreira

Classification: Internal – Confidential

CRA Control: CRA 34.1.1

---

1. Purpose

This Standard defines how Synthetic Users identifies, classifies, stores, retains, and disposes of records throughout their lifecycle. It ensures that information assets are managed in a manner consistent with legal, regulatory, and contractual obligations — including obligations arising from the JPMC client engagement — and that records are available for audit and compliance purposes.

This Standard supplements (and is distinct from) the Records & Document Management Policy, which covers the operational management of policy documents and internal working documents.

---

2. Scope

This Standard applies to:

- All records created, received, or maintained by Synthetic Users in the course of business operations
- All employees, contractors, and third parties who create, store, or process Synthetic Users records
- All systems used to store Synthetic Users records, including cloud storage, databases, communication platforms, and AI/GenAI system logs

---

3. Information Classification

All records and information assets are classified into one of four levels:

Classification	Description	Examples	Access
Highly Confidential	Records containing customer PII, JPMC data, security findings, credentials, or legal holds	JPMC study data, penetration test reports, encryption keys, legal hold records, breach notifications	Named individuals only; strict need-to-know
Confidential	Internal business records not for external disclosure	Financial statements, contracts, HR records, internal audit reports, vendor DPAs	Internal staff with business need
Internal	General operational records shared within the organization	Meeting notes, project plans, operational procedures, internal communications	All employees and approved contractors
Public	Records approved for external publication	Privacy policy, terms of service, public security documentation	No restriction

Classification is assigned at creation and reviewed when records are transferred or retained beyond their initial period.

---

4. Records Lifecycle

4.1 Creation

- Records are created in the appropriate system based on their classification and type
- Each record must have a clear title, creation date, and owner
- AI/GenAI-generated content is labelled as such at creation (see Section 8)

4.2 Storage & Access

- Highly Confidential and Confidential records are stored in access-controlled systems with encryption at rest (AES-256)
- Access is granted on a least-privilege, need-to-know basis
- Shared access to Confidential records requires documented justification
- JPMC-specific records are stored in designated, isolated storage locations

4.3 Use & Transmission

- Records are transmitted externally only over encrypted channels (TLS 1.2+)
- Highly Confidential records may not be transmitted via personal email, personal cloud storage, or unencrypted channels
- Records shared with JPMC are provided through approved channels only

4.4 Retention

Retention periods are defined in Section 6. Records are retained in accordance with their classification and type, taking into account the longer of: the business need, the legal requirement, and any applicable contractual obligation.

4.5 Disposal

Records are disposed of in accordance with the disposal methods defined in Section 7. Disposal is documented and approved per the requirements of each classification level.

5. Retention Schedule

Record Category	Record Types	Retention Period	Legal Basis	Primary Storage System
Customer Data	Study configurations, interview transcripts, synthetic outputs, personas	Duration of customer relationship + 30 days (unless legally required to retain)	Contract; GDPR Art. 5	Customer database partition (PostgreSQL / AWS RDS)
JPMC Client Data	JPMC study data, outputs, correspondence	Duration of engagement + 3 years	JPMC contractual requirements	Isolated JPMC storage; legal folder
Financial Records	Invoices, receipts, bank records, payroll, tax filings	7 years	Tax and corporate law	Accounting system; CFO secure folder
Contracts & Legal	Vendor contracts, NDAs, DPAs, employment agreements, client agreements	Duration of contract + 7 years	Contract law; applicable statute of limitations	Legal documentation repository (Git-backed)
Security & Compliance Records	SOC 2 reports, penetration test reports, vulnerability scans, SAST reports, risk assessments	3 years	SOC 2; contractual (JPMC)	Compliance folder; legal documentation repository

AI/GenAI Records	Model validation checklists, AI risk assessments, adversarial test reports, provider DPAs	3 years	JPMC SCA CRA 13.1.1; contractual	Internal compliance folder; legal folder
HR & Employment Records	Offer letters, performance reviews, training records, termination documents	Duration of employment + 7 years	Employment law	HR system; CEO secure folder
Operational Records	Meeting notes, project plans, internal communications	2 years (unless escalated to Confidential status)	Business need	Notion; email systems
Incident Records	Incident reports, post-mortems, breach notifications, remediation evidence	5 years	GDPR Art. 33; contractual	Incident management system; legal folder
Audit Logs & Access Logs	System access logs, API logs, change management logs, authentication events	1 year rolling (extended to 3 years if security incident occurs)	SOC 2; contractual	AWS CloudWatch; logging service

6. Extended Retention — Legal Hold

When Synthetic Users receives a legal hold notice or anticipates litigation, regulatory inquiry, or JPMC-related investigation:

1. The CEO and Legal advisor are notified immediately
2. A legal hold is placed on all potentially relevant records — standard disposition schedules are suspended for affected records
3. Affected records are identified, preserved, and labelled with the legal hold reference
4. Records under legal hold are stored in a designated, access-controlled location
5. The legal hold is reviewed quarterly and lifted only with CEO + Legal advisor approval
6. When lifted, normal retention and disposal schedules resume for the affected records

7. Disposal Methods

Disposal Method	When Used	Evidence Required
Cryptographic erasure	Cloud-stored data (S3, RDS) where re-keying or key deletion renders data inaccessible	Deletion confirmation from cloud provider or key management log
Secure deletion (software)	Application-level data deletion from databases and file stores	Deletion log entry; developer confirmation
Database record purge	Structured data subject to retention expiry (e.g., customer data post-contract)	Automated purge job log
Certified destruction (third-party)	Any physical media (not currently applicable — Synthetic Users operates cloud-only)	Certificate of destruction
Provider data deletion	AI/GenAI provider data upon decommissioning	Written confirmation from provider per DPA

confirmation		
Archive and tombstone	Records that must be retained for legal hold but removed from active systems	Archive log; tombstone record in source system
Document shredding	Any physical documents (rare; applies to printed contracts or physical mail)	Destruction log
Degaussing / physical destruction	Physical storage media (if any)	Certificate of destruction

Disposal of Highly Confidential records requires CTO approval and written documentation.

---

8. AI/GenAI Records

AI/GenAI systems at Synthetic Users generate records that require specific governance:

Record Type	Labelling	Retention	Notes
AI-generated interview responses	`type: ai_generated` in database; labelled in UI	Per customer data retention	Not presented as human responses
AI-generated research reports	Prominently labelled "AI-Generated Synthesis" in UI	Per customer data retention	Attribution chain preserved
Prompt template versions	Tagged in Git repository	3 years	Version history preserved in Git
Inference logs (application-level)	Tagged with session ID; no PII in logs	1 year rolling	Scoped to tenant

Model validation records	Stored in compliance folder	3 years	Required by JPMC CRA 13.1.1
AI/GenAI risk assessment records	Stored in compliance folder	3 years	Required by JPMC CRA 13.1.1

9. Roles and Responsibilities

Role	Responsibility
CTO — Artur Ventura	Standard owner; approves disposal of Highly Confidential records; oversees AI/GenAI records governance
CFO — Zumbi Ferreira	Owns financial records retention; approves disposal of financial records
CEO — Kwame Ferreira	Approves legal holds; approves policy exceptions; receives disposal confirmation for JPMC records
All Employees	Responsible for classifying records they create; adhering to retention schedules; reporting disposal of records not yet past their retention period
Engineering Team	Implements technical controls for retention and disposal in platform systems; maintains audit logs

10. Change Management

Version	Date	Author	Summary

1.0	March 25, 2026	Artur Ventura, CTO	Initial release. Establishes classification scheme, full retention schedule, disposal methods, AI/GenAI records section, and legal hold procedure in response to JPMC CRA 34.1.1.

11. Review

This Standard is reviewed annually or whenever a material change occurs to applicable law, contractual obligations, or system architecture. Updates require CTO approval.

12. Related Documents

- Records & Document Management Policy
- User Data Deletion & Retention Policy
- AI/GenAI Decommissioning Policy
- SDLC AI/GenAI Addendum
- Privacy Policy
- Incident Response Plan

Synthetic Users, Inc. — 4223 Glencoe Ave, Suite C215-523, Marina del Rey CA 90292