Synthetic Users Third-Party Risk Management Policy

Version: 2.0

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 19.1.3

Change History

Version	Date	Author	Changes
1.0	January 7, 2025	Security & Compliance Lead	Initial release
2.0	March 25, 2026	Artur Ventura, CTO	Added formal risk tier classification (HIGH / MEDIUM / LOW) with JPMC-required factors; added full subcontractor risk register (19 vendors); added due diligence requirements by tier; added monitoring frequency table. Updated per JPMC SCA CRA 19.1.3.

1. Purpose

The purpose of this policy is to ensure that all third parties and vendors engaged by Synthetic Users maintain security, privacy, and compliance standards consistent with our internal controls and regulatory obligations — including those required by JPMC under the Security Controls Assessment (SCA). This policy defines how Synthetic Users assesses, categorizes, monitors, and manages third-party risks throughout the full vendor lifecycle.

2. Scope

This policy applies to all third parties that store, process, or access Synthetic Users' company data, customer data, or production systems. It includes service providers, SaaS vendors, infrastructure platforms, AI/GenAI model providers, consultants, and open-source dependencies used within Synthetic Users' environment.

3. Objectives

- Identify and mitigate risks associated with third-party relationships
- Ensure vendors comply with SOC 2, GDPR, and other relevant standards
- Maintain accountability and visibility across the vendor ecosystem
- Apply formal risk tier classification (HIGH / MEDIUM / LOW) to all active subcontractors
- Enforce contractual and technical safeguards for data protection
- Meet JPMC SCA CRA 19.1.3 requirements for subcontractor risk management

4. Roles and Responsibilities

Role	Responsibility
CTO — Artur Ventura	Policy owner; oversees vendor risk assessments; approves onboarding of HIGH-risk vendors; manages AI/GenAI provider risk
CFO — Zumbi Ferreira	Approves financial and commercial vendor commitments; ensures DPAs are in place for data-processing vendors
Engineering & Product Teams	Identify and review technical dependencies (SaaS tools, APIs, SDKs); flag new third-party integrations
CEO — Kwame Ferreira	Final approval for HIGH-risk vendor onboarding; notified of vendor-related security incidents affecting JPMC engagement

5. Risk Tier Classification

5.1 Tier Definitions

Vendors are assigned a risk tier based on the following JPMC-required factors:

Factor	HIGH	MEDIUM	LOW
Data Sensitivity	Processes customer PII, JPMC data, or production secrets	Processes internal business data (non-customer, non-JPMC)	No access to sensitive data
System Access	Direct access to production systems or infrastructure	Access to internal tools or business systems	No access to production or business systems

Business Criticality	Outage causes platform downtime or data loss	Outage causes operational disruption but no data loss	Outage has minimal business impact
Volume of Data	Large volumes of customer or regulated data	Moderate volumes of internal data	Minimal or no data processed
Regulatory Scope	In scope for GDPR, CCPA, SOC 2, or JPMC contractual obligations	Partial scope (e.g., internal data only)	Not in regulatory scope
Data Residency	Processes or stores data in jurisdictions requiring contractual controls	Data residency in primary operating countries	No data residency concerns
Subcontracting	Subcontracts to further parties with access to sensitive data	Limited subcontracting	No further subcontracting

6. Subcontractor Risk Register

All active Synthetic Users subcontractors and their assigned risk tiers are documented below. This register is reviewed and updated annually.

Last reviewed: March 25, 2026

6.1 HIGH Risk Subcontractors

Vendor	Service	Data/Access	Certifications	DPA	Review Frequency
Amazon Web	Cloud infrastructure	Customer PII,	SOC 2 Type II, ISO 27001,	Yes	Annual

Services (AWS)	(compute, storage, database, networking)	production data, JPMC study data	PCI DSS		
Render	Application hosting, environment configuration, deployment	Production application, environment variables, secrets	SOC 2 Type II	Yes	Annual
OpenAI	LLM inference API (via LLM Shuffle)	Prompt data including customer context; output data	SOC 2 Type II	Yes (no training on API data)	Annual
Anthropic	LLM inference API (Claude, via LLM Shuffle)	Prompt data including customer context; output data	SOC 2 Type II	Yes (no training on API data)	Annual
Google Cloud / Gemini	LLM inference API (via LLM Shuffle); embedding services	Prompt data; embedding inputs	SOC 2 Type II, ISO 27001	Yes	Annual
Google Firebase	Application user authentication and identity management	User credentials, session tokens, MFA events	SOC 2 Type II, ISO 27001	Yes	Annual

Google Workspace	Employee identity management, SSO, MFA, email, collaboration	Employee credentials, session tokens, MFA events, corporate email	SOC 2 Type II, ISO 27001	Yes (DPA)	Annual
GitHub	Source code repository, CI/CD, security scanning	Proprietary source code, secrets scanning, deployment pipelines	SOC 2 Type II	Yes	Annual

6.2 MEDIUM Risk Subcontractors

Vendor	Service	Data/Access	Certifications	DPA	Review Frequency
Stripe	Payment processing	Payment card data (Stripe handles PCI compliance; Synthetic Users does not store card data)	PCI DSS Level 1, SOC 2	Yes	Annual
Notion	Internal documentation and operations	Internal business data, operational records	SOC 2 Type II	Yes	Annual
Intercom	Customer communications	Customer email	SOC 2 Type II	Yes	Annual

	and support	addresses, support conversation content			
1Password	Credential and secret management	Employee passwords, API keys, service credentials	SOC 2 Type II	Yes	Annual
Mistral AI	LLM inference API (via LLM Shuffle)	Prompt data	EU AI Act alignment; DPA	Yes	Annual

6.3 LOW Risk Subcontractors

Vendor	Service	Data/Access	DPA	Review Frequency
Vercel / Netlify	Static asset hosting (if applicable)	No PII; public static files only	N/A	Bi-annual
Linear	Engineering project management	Internal task data; no customer PII	N/A	Bi-annual
Loom	Internal video recording	Internal communications only	N/A	Bi-annual
Figma	Design tooling	Product designs; no customer PII	N/A	Bi-annual
Slack	Internal team communication	Internal messages; no production system access	SOC 2	Yes
Calendly / scheduling tools	Meeting scheduling	Contact emails; no PII beyond scheduling	N/A	Bi-annual

Google Workspace	Email, docs, calendar	Internal communications; employee data	Yes	Annual

7. Due Diligence Requirements by Tier

Requirement	HIGH	MEDIUM	LOW
Third-Party Risk Assessment (TPRA)	Required before onboarding	Required before onboarding	Not required
SOC 2 / ISO 27001 / equivalent review	Required; must be current (< 12 months)	Required if available	Not required
Data Processing Agreement (DPA)	Required	Required if personal data involved	Not required
Encryption verification (in transit + at rest)	Required	Required	Not required
Incident response SLA review	Required	Recommended	Not required
Subcontractor disclosure review	Required	Recommended	Not required
CEO approval for onboarding	Required	CTO approval sufficient	CTO awareness
Annual security questionnaire	Required	Recommended	Not required

8. Vendor Risk Management Lifecycle

8.1 Identification

- All new third-party engagements must be reported to the CTO before contract signing or data exchange
- New vendors are assigned a risk tier before any data sharing or system access is granted

8.2 Due Diligence and Assessment

A Third-Party Risk Assessment (TPRA) is conducted prior to onboarding HIGH and MEDIUM risk vendors. Assessment includes:

- Review of SOC 2, ISO 27001, or equivalent certifications
- Verification of encryption, access control, and data protection measures
- Evaluation of incident response and breach notification procedures
- Review of subcontractor and data residency arrangements
- For AI/GenAI providers: review of data retention, training opt-out, and prompt logging practices

8.3 Contractual Requirements

All HIGH and MEDIUM risk vendor contracts must include:

- A Data Processing Agreement (DPA) where personal data is involved
- Confidentiality and non-disclosure clauses
- Clear obligations for data protection, breach notification (72 hours), and deletion upon termination
- Right to audit or require attestation reports (e.g., SOC 2 Type II)

8.4 Ongoing Monitoring

Risk Tier	Review Frequency	Activities
HIGH	Annual	Full TPRA review; DPA reconfirmation; SOC 2 / certification update; security questionnaire
MEDIUM	Annual (or upon material change)	DPA reconfirmation; certification check
LOW	Bi-annual	Confirm service is still in use; confirm no change in data access

Continuous monitoring of open-source dependencies via Dependabot. Vendor incident notifications tracked and reviewed to assess downstream impact.

8.5 Offboarding

Upon termination of any vendor relationship, Synthetic Users ensures:

- All customer and company data is deleted or returned securely
- A Certificate of Data Destruction or written confirmation is obtained for HIGH-risk vendors
- System credentials and access are immediately revoked
- The subcontractor risk register is updated

---

9. Reporting and Escalation

- Any vendor-related incident or suspected breach must be reported immediately to the CTO
- If customer data or JPMC data is affected, the Incident Response Plan is triggered and the CEO is notified
- Major vendor risks are reported to the Executive Team during quarterly security reviews

---

10. Policy Review and Maintenance

This policy is reviewed annually or following any major vendor onboarding, breach, or regulatory update. Updates require approval from the CTO and CEO.

11. Related Documents

- AI/GenAI Algorithm Design Document
- AI/GenAI Decommissioning Policy
- Information Governance & Records Management Standard
- Encryption Policy
- Incident Response Plan
- Privacy Policy
- Subprocessors & Data Flow

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