Synthetic Users Technology Asset Management Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy establishes a framework for identifying, tracking, managing, and securing all technology assets used by Synthetic Users to deliver its services.

2. Scope

This policy covers all technology assets including:

- Cloud infrastructure resources (compute, storage, networking)
- SaaS and third-party services
- Employee workstations and devices
- Software licenses and subscriptions
- Domain names, certificates, and cryptographic keys

3. Asset Inventory

3.1 Cloud Infrastructure Assets

Synthetic Users maintains a cloud-native infrastructure. All production assets are provisioned and tracked through the following platforms:

Platform	Purpose	Asset Tracking Method
AWS	Hosting, storage (S3), compute (EC2)	AWS Console, resource tagging
Render	Application hosting, managed services	Render Dashboard
Vercel	Frontend hosting	Vercel Dashboard
Cloudflare	CDN, WAF, DNS	Cloudflare Dashboard

All cloud resources are tagged with environment (production, staging), service name, and owner.

3.2 SaaS and Third-Party Services

All third-party services are documented in the Subprocessors and Data Flow registry. Each service is categorized as core infrastructure or additional service, with purpose and data location documented.

3.3 Employee Devices

- All employee workstations are Apple MacBooks, registered and monitored through our Sprinto.
- Device inventory includes hardware serial number, assigned user, operating system version, and compliance status.
- Devices must have full disk encryption (FileVault) and anti-malware (macOS built-in protections) enabled and verified.

3.4 Software and Licenses

- Software licenses are tracked centrally and reviewed during access rights reviews.
- Only approved software may be installed on employee devices.

---

4. Asset Lifecycle Management

4.1 Provisioning

- New cloud resources are provisioned through documented infrastructure-as-code processes or managed platform dashboards.
- New employee devices are configured according to the baseline security configuration before being issued.

4.2 Monitoring

- Cloud assets are monitored for availability, performance, and security through centralized logging (Axiom, PaperTrail).
- Endpoint compliance (FDE, anti-malware, OS updates) is monitored through Sprinto (Dr. Sprinto MDM).

4.3 Recertification

- Cloud infrastructure assets are reviewed quarterly as part of firewall and security group reviews.
- Employee device compliance is verified continuously through monitoring tooling.
- Third-party services are reviewed annually per the Third-Party Risk Management Policy.

4.4 Decommissioning

- Cloud resources no longer in use are deprovisioned and removed from the inventory.
- Employee devices are securely wiped before reassignment or disposal per the Data Deletion and Retention Policy.

- Access to decommissioned services is revoked within 24 hours.

5. Roles and Responsibilities

Role	Responsibility
CTO	Policy approval, overall accountability
Security & Compliance Lead	Maintain asset inventory, conduct reviews
Engineering Team	Tag and document cloud resources, report changes
All Employees	Report lost/stolen devices, comply with device policies

6. Review

This policy is reviewed annually or when significant changes to the technology environment occur.