Synthetic Users Remote Access Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines how Synthetic Users secures remote access to corporate and production systems using a Zero Trust approach, without reliance on traditional VPN technology.

2. Scope

This policy applies to all employees, contractors, and systems that access Synthetic Users corporate or production environments remotely.

3. Zero Trust Access Model

Synthetic Users does not use VPN technology. Instead, all remote access is secured through a Zero Trust architecture based on the following principles:

1. **Never trust, always verify** — Every access request is authenticated and authorized regardless of network location.
2. **Least privilege** — Users receive only the minimum access required for their role.

3. **Continuous verification** — Access is re-evaluated based on identity, device posture, and context.

---

4. Authentication Controls

4.1 Single Sign-On (SSO)

- All access to corporate systems (Google Workspace) and production systems is authenticated through SSO.
- SSO is configured via SAML 2.0 or OpenID Connect.

4.2 Multi-Factor Authentication (MFA)

- MFA is mandatory for all accounts — both corporate (Google Workspace) and production/backend access.
- MFA is enforced at the identity provider level.

4.3 No Shared Credentials

- Each user has a unique identity. Shared accounts or credentials are prohibited.
- Service accounts use scoped API keys or OAuth tokens with minimum required permissions.

---

5. Device Requirements

- Only company-managed Apple MacBooks are authorized to access corporate and production systems.
- Devices must be compliant with the Endpoint Security Policy, including full disk encryption and anti-malware.
- Device compliance is monitored through Sprinto (Dr. Sprinto MDM).

---

6. Network Security

6.1 No VPN / No Split Tunneling

- As Synthetic Users does not use VPN technology, split tunneling is not applicable.
- All application access occurs over HTTPS (TLS 1.2+) directly to cloud-hosted services.
- There is no corporate network perimeter to bypass — the identity layer is the security boundary.

6.2 Cloud-Native Security

- Production infrastructure is protected by AWS Security Groups, Render network isolation, and Cloudflare WAF.
- Administrative access to cloud platforms requires individual accounts with MFA.
- SSH access to servers is disabled; all management is through managed platform dashboards.

7. Access Logging and Monitoring

- All authentication events are logged centrally.
- Failed authentication attempts trigger alerts.
- Access logs are retained for 12 months.

8. Review

This policy is reviewed annually or when changes to the access architecture occur.