Synthetic Users Security Configuration 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, monitors, and maintains secure configurations across its infrastructure and application environments.

2. Scope

This policy applies to all production and staging environments, including cloud infrastructure, application containers, and managed services.

3. Configuration Management Approach

Synthetic Users operates a **fully managed, containerized infrastructure**. This architecture eliminates traditional server configuration management concerns:

- **No self-managed servers** — All compute runs on managed platforms (Render, AWS managed services) where the provider is responsible for OS patching, kernel updates, and base infrastructure security.

- **Immutable containers** — Applications are deployed as container images. Containers are not modified after deployment; changes require building and deploying a new image.
- **No SSH access** — Server-level access is disabled. All management is performed through managed platform dashboards and APIs.

---

4. Configuration Controls

4.1 Application Configuration

- All application environment variables and configuration are managed through **Render's configuration platform**.
- Configuration changes follow the Change Management Policy, requiring documentation and peer review.
- Secrets and credentials are stored in Render's encrypted environment variable system, not in source code.

4.2 Infrastructure Configuration

Component	Configuration Method	Drift Risk
Compute (containers)	Immutable container images	None — containers are replaced, not modified
Networking (AWS)	Security Groups, NACLs	Reviewed quarterly
DNS / Edge (Cloudflare)	Cloudflare dashboard	Changes logged by Cloudflare
Storage (S3)	Bucket policies, IAM	Reviewed quarterly

4.3 Source Code & Dependencies

- All source code is managed in Git with branch protection and peer review requirements.

- Dependencies are tracked and scanned for known vulnerabilities as part of the SDLC.
- GitHub secret scanning prevents accidental commit of credentials.

5. Configuration Baseline Compliance

- Container images are built from standard, minimal base images.
- Non-essential services, ports, and packages are not included in container images.
- Default credentials are never used; all authentication is through SSO/MFA or scoped API keys.
- Baseline configuration settings for the application are documented in Baseline Configuration Settings.

6. Monitoring

- Render and AWS provide audit logs for all configuration changes.
- Cloudflare logs all DNS, WAF, and network configuration changes.
- Unauthorized configuration changes would require compromising the managed platform account, which is protected by SSO with MFA.

7. Review

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