

Network Security and Environment Isolation Standard

Owner	Andrew Smith, Security Owner
Version	1.1, effective October 19, 2026
Part of	Swapt Information Security Policy

1. Architecture overview

- **Application.** The Swapt application runs as containers on Google Cloud App Engine (flexible environment), a managed platform. Google operates and patches the underlying hosts and network, and no Swapt staff have shell access to production hosts.
- **Database.** Production data is stored in a managed PostgreSQL database on Google Cloud SQL, with automated daily backups. Access requires dedicated database credentials, held only in the production platform's secret configuration.
- **Edge.** Public traffic reaches Swapt only over HTTPS through managed edge networks (Google Cloud load balancing, Amazon CloudFront and Cloudflare). These provide TLS termination and DDoS mitigation.
- **Storage.** Files and images are stored in Cloudflare R2 object storage. Access requires API keys held only by the application.
- **Background work.** Scheduled and long-running jobs run on Temporal, over authenticated and encrypted connections.

2. Environment isolation

- Production, development and test environments are fully separate. Each has its own database, credentials and configuration.
- Development runs on engineers' encrypted laptops against local databases. Automated tests run against a throwaway local database with dummy credentials.
- Production personal data is never copied into development or test environments.
- Production credentials are stored only in the production platform's secret configuration. They are never committed to source control, and they are available only to the people listed in the access register (see the Access Control Policy).

3. Network segmentation and perimeter protection

- All user and partner traffic is served over HTTPS only. HTTP requests are redirected to HTTPS, and HTTP Strict Transport Security (HSTS) is enabled.

- Administrative access to cloud resources happens only through the providers' consoles and CLIs, which require MFA, and is limited to the people listed in the access register.
- Inbound webhooks from partners (TikTok Shop, Shopify) are accepted only after their signatures are verified.
- The application enforces rate limits on login, password reset, magic links and public endpoints to slow brute-force and abuse attempts.
- Session cookies are HTTP-only, Secure and SameSite=Lax. Pages cannot be framed by other sites (X-Frame-Options: DENY), and browsers are told not to guess content types.

4. Monitoring and threat detection

- Application errors and unusual failures are captured in Sentry and alert the engineering team.
- Platform request logs and audit logs from Google Cloud, AWS and Cloudflare record administrative actions and traffic, and are reviewed when investigating suspicious activity.
- Cloudflare and CloudFront provide automatic DDoS protection at the edge.
- Suspected network threats are handled under the Incident Response Plan.

5. Review

The Security Owner reviews network and firewall settings, including database network access rules, every quarter and after any infrastructure change, and records the review in the security log.