

Swapt Information Security Policy

Document owner	Andrew Smith, Security Owner (andrew@swaptqr.com)
Version	1.1
Effective date	October 19, 2026
Review cycle	At least once a year, and after any significant incident or change to our systems
Applies to	All Swapt employees, contractors, systems and data

1. Purpose

This policy sets out how Swapt protects the confidentiality, integrity and availability of the information we hold. That includes our customers' (sellers') data, the data of buyers who opt in through sellers' Swapt pages, and data we receive from partner platforms such as TikTok Shop, Shopify and Amazon.

2. Scope

This policy covers:

- The Swapt web application, its APIs, background workers and databases.
- Cloud infrastructure: Google Cloud Platform (application hosting and PostgreSQL database), Cloudflare (storage, CDN and network protection), Amazon Web Services (CloudFront and SES email delivery) and Temporal (background job orchestration).
- Company accounts: Google Workspace, GitHub, cloud consoles and other SaaS tools.
- Company laptops and any device used to access Swapt systems or data.
- Everyone with access to the above: employees, contractors and service providers.

3. Roles and responsibilities

- **Security Owner (Andrew Smith).** Owns this policy and the supporting standards. Approves access to production systems, leads incident response, runs access reviews and tracks vulnerabilities to closure.
- **Engineers.** Follow secure development practices, keep dependencies up to date, and report suspected security issues immediately.
- **All personnel.** Follow this policy, protect their credentials and devices, and report suspected incidents to the Security Owner without delay.

4. Policy statements

Swapt maintains the following supporting standards. Each one is part of this policy and is binding.

Area	Supporting document
Network security, environment isolation and perimeter protection	Network Security and Environment Isolation Standard
Anti-malware and endpoint protection	Endpoint Protection Standard
Workstation and account security baseline	Security Baseline Standard
Access control and least privilege	Access Control Policy
Data classification and encryption	Data Classification and Encryption Policy
Incident response	Incident Response Plan
Vulnerability and patch management	Vulnerability and Patch Management Procedure
Personal data protection, data subject requests and retention	Personal Data Protection Policy

In summary:

1. **Least privilege.** People and systems get only the access they need. Production access is limited to named engineers and is reviewed every quarter.
2. **Strong authentication.** Multi-factor authentication is required on Google Workspace, GitHub, Google Cloud, AWS, Cloudflare and every other administrative console.
3. **Encryption.** All traffic between users, partners and Swapt is encrypted with TLS 1.2 or higher, and all stored data is encrypted at rest. Partner API credentials, such as TikTok Shop access and refresh tokens, are additionally encrypted by the application with AES-256.
4. **Data minimization.** We collect and keep only the data the service needs. From TikTok Shop we read only product, SKU and order-status data. We do not read buyer names, addresses or contact details from TikTok Shop, and we use TikTok Shop data only to provide the service to the seller who authorized it.
5. **Environment separation.** Development and test environments are separate from production and never contain production personal data.
6. **Secure development.** All code changes go through pull requests with review before release. Secrets are kept out of source code.
7. **Monitoring.** Application errors and performance are monitored continuously with Sentry and platform logs.
8. **Vulnerability management.** Dependencies are checked for known vulnerabilities and patched within defined timeframes.
9. **Incident response.** Incidents are handled under the Incident Response Plan. Affected sellers and partners, including TikTok Shop, are notified without undue delay and within 72 hours of confirming a

breach that involves their data.

10. **Vendor management.** We use only reputable infrastructure providers that maintain recognized security certifications (such as SOC 2 and ISO 27001), and we review their security posture when we adopt them.
11. **Data subject rights and retention.** We help sellers and partners respond to requests to access, correct or delete personal data. When a seller's contract ends, we revoke their partner tokens immediately and delete their customer data within 30 days, unless the law requires us to keep it.

5. Personnel security

- Everyone with system access acknowledges this policy when they join and after each annual update.
- Access is removed on the day a person leaves or no longer needs it.
- Personnel receive security awareness guidance when they join and at least once a year, covering phishing, credential handling and incident reporting.

6. Compliance and exceptions

Breaking this policy may lead to access being removed and disciplinary action. Any exception must be approved in writing by the Security Owner, with an expiry date and compensating controls, and is recorded in the security log.

7. Review

The Security Owner reviews this policy and every supporting standard at least once a year, and after any significant incident or change to our infrastructure.