

# Access Control Policy

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

## 1. Principles

- **Least privilege.** People and services get only the minimum access their role needs, for only as long as they need it.
- **Need to know.** Personal data, including any data received from TikTok Shop, is accessed only to provide or support the service for the seller who authorized it.
- **Named accounts.** Every account belongs to one identified person or service. Shared personal logins are not allowed.
- **Authentication.** Every administrative account requires MFA (see the Security Baseline Standard).

## 2. Role-based access: internal systems

| Role                           | Who                     | Access                                                                                                                                        |
|--------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Security Owner / Administrator | Andrew Smith            | Administrative access to cloud consoles, production configuration and the database; approves all access                                       |
| Engineer                       | Named engineering staff | Source code; production deploys through the approved pipeline; production data only when needed to investigate an incident or support request |
| Support / Operations           | Named staff             | The Swapt admin interface for assigned seller accounts; no direct database or infrastructure access                                           |
| Contractors                    | As approved             | Time-limited, scoped to the specific task, removed when the task ends                                                                         |

The Security Owner keeps a register of who holds production, database and cloud console access.

## 3. Role-based access: the Swapt application

- **Tenant isolation.** Each seller's data belongs to their organization. Every application query is scoped to the signed-in user's organization, so one seller can never see another seller's data.
- **Roles within a seller account.** Account administrators can manage settings, users and integrations. Other users get the narrower roles, including view-only access, that their administrator assigns.

- **Internal admin functions.** Super-admin access requires signing in with one of a short allowlist of company Google accounts, with Google 2-Step Verification. There is no shared admin password.
- **No anonymous access to data.** Endpoints that hand out promo codes, prize files or customer form data require a signed-in session or the customer's own access token, and are limited to the caller's organization. Automated tests check these guards on every change.
- **Least-privilege service accounts.** Components get only the database permissions they need. For example, the reporting assistant uses a dedicated database role with read-only access to an approved set of tables and a statement time limit.
- **Partner credentials.** TikTok Shop access and refresh tokens are encrypted by the application and used only by the server to read product and order-status data for the authorizing seller. They are never shown in the user interface or logs.

## 4. Granting, changing and removing access

1. Access requests go to the Security Owner, stating the role and the reason.
2. The Security Owner approves the minimum access needed and records it in the access register.
3. When someone's role changes, the access they no longer need is removed.
4. When someone leaves, all their access is removed on their last day: Google Workspace, GitHub, cloud consoles, the password manager and the Swapt admin. Shared secrets they could see are rotated.

## 5. Access reviews

- Every quarter, the Security Owner reviews everyone with access to Google Cloud, AWS, Cloudflare, GitHub, the production database and the Swapt super-admin.
- Access that is no longer needed is removed immediately.
- Each review is recorded in the security log with its date, who reviewed it, what was found and what changed.

## 6. Logging

Administrative actions in Google Cloud, AWS, Cloudflare and GitHub are recorded in those providers' audit logs. Super-admin sign-ins to seller accounts are flagged in the application.