

Data Classification and Encryption Policy

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

1. Data classification

Class	Examples	Handling
Restricted	Partner API credentials (TikTok Shop, Shopify, Amazon tokens), application secrets, password hashes, data received from partner APIs	Encrypted at rest, plus application-level encryption for credentials, so they stay encrypted wherever they are stored or sent internally; access limited to the application and the Security Owner; never logged or exported
Confidential	Personal data of buyers who opt in (name, email, phone if provided), seller account data, order references	TLS between users and Swapt; encrypted at rest; access limited to the owning seller and authorized staff; processed only to provide the service
Internal	Business documents, source code, configuration without secrets	Company accounts with MFA; not shared outside Swapt without approval
Public	Marketing website and published documentation	No restriction

Data from TikTok Shop is classified **Restricted** and used only to provide the service to the seller who authorized it. Swapt reads product, SKU and order-status data, and does not read buyer names, addresses or contact details from TikTok Shop.

2. Encryption in transit

- All traffic between users, partners and Swapt uses HTTPS with TLS 1.2 or higher. Plain HTTP is redirected to HTTPS, and HSTS tells browsers to connect only over HTTPS.
- All calls from Swapt to partner and provider APIs (TikTok Shop, Shopify, Amazon, AWS SES, Cloudflare R2, Temporal) use TLS.
- Session cookies carry the Secure flag, so browsers send them only over HTTPS.
- Email is delivered through AWS SES, which uses TLS to connect to receiving mail servers whenever they support it.

3. Encryption at rest

- **Database.** The production PostgreSQL database on Google Cloud, including its backups, is encrypted at rest with AES-256 by Google Cloud.
- **File storage.** Files in Cloudflare R2 are encrypted at rest with AES-256 by Cloudflare.
- **Application-level encryption.** Restricted credentials, including TikTok Shop access and refresh tokens and other integration secrets, are encrypted by the application with AES-256-CBC and an HMAC-SHA256 integrity check before they are written to the database. A database copy alone therefore does not reveal them.
- **Passwords.** User passwords are stored only as salted scrypt hashes.
- **Endpoints.** Every company laptop uses FileVault full-disk encryption.

4. Key management

- Encryption keys for data at rest in Google Cloud and Cloudflare are managed by those providers' key management services.
- The application encryption key is stored only in the production platform's secret configuration, not in source code, and is available only to the Security Owner.
- Keys and secrets are rotated if they may have been exposed, and when people with access to them leave.

5. Retention and disposal

- Personal data is kept only as long as the seller's account is active, or as the seller instructs.
- When a seller's contract ends, their partner tokens are revoked and deleted immediately, and their customer data is deleted within 30 days unless the law requires us to keep it.
- Requests to access, correct or delete a person's data are handled within 30 days.