Scan2Tray

Data Classification & Encryption Standard

Scan2Tray Ltd (Company No. 17096824) · Version 1.0 · 24 September 2026 · Owner: Paul Hinett, Director · hello@scan2tray.com

Supplement to the Scan2Tray Information Security Policy.

1. Classification

All information Scan2Tray handles falls into one of four classes. The class determines how it is stored, transmitted, shared and disposed of.

Class	Examples	Handling
Restricted	Marketplace OAuth access/refresh tokens and shop ciphers; application signing keys; database and provider credentials; payment provider keys.	Held only server-side as environment variables or encrypted database fields. Never logged, never sent to clients, never stored on endpoints or in source control. Rotated on suspicion of exposure.
Confidential	Seller account data (name, email, phone, hashed password); marketplace order data including buyer identifiers, buyer display names, addresses on uploaded shipping labels, tracking numbers and prices.	Accessible only through authenticated, organisation-scoped endpoints. Not printed or kept on paper. Shared with third parties only as required to provide the service. Deleted on request within 30 days.
Internal	Application and proxy logs, scan events, diagnostics, metrics.	Secrets and tokens redacted before logging. Retained for the shortest useful period (diagnostics 14 days, proxy logs about 7 days).
Public	Marketing site content, published policies, product documentation.	No restrictions.

2. Encryption in transit

- All traffic between users, marketplaces and Scan2Tray services uses HTTPS with TLS 1.2 or higher, terminated at a single reverse proxy with automatically renewed certificates. Plain HTTP is not served.
- All outbound calls to marketplace APIs, Stripe, email and speech providers use HTTPS.
- Administrative access uses SSH over a private WireGuard overlay network; database connections from staff traverse that encrypted overlay.
- Traffic between containers on the production host does not leave the host and travels only on isolated internal Docker networks.

3. Encryption at rest

Data	Protection
Marketplace OAuth tokens (Restricted)	Encrypted at the application layer with AES-256-GCM and a per-value random nonce before being written to the database. The key is held only in the API's runtime configuration, so a database export alone cannot yield usable credentials.
Seller passwords (Confidential)	Never stored; only salted BCrypt hashes.
Application secrets (Restricted)	Environment variables on the deployment platform; not written to disk in source or configuration files.

Staff endpoints	Full-disk encryption (FileVault on macOS, BitLocker on Windows) as required by the Endpoint Security Standard.
Production database and label-file storage (Confidential)	Reside on an access-controlled volume reachable only from the application containers and the private administration network, in a provider data centre with ISO 27001 physical controls. Block-level encryption of this volume is scheduled for Q4 2026.
Backups	Stored separately from the live database with the same access restrictions; retained for at least 30 days.

4. Disposal

- Seller accounts and data are deleted on request within 30 days, subject to legal retention of billing records.
- Marketplace tokens are invalidated the moment a seller disconnects or revokes the app.
- Decommissioned servers are wiped by the provider on deletion; replaced endpoints are erased before disposal.

5. Review

This standard is reviewed with the Information Security Policy at least annually and whenever a new class of data or a new storage location is introduced.