Scan2Tray

Access Control Policy

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. Purpose and principles

This policy governs who can access Scan2Tray systems and the personal data they hold, and how that access is granted, used, reviewed and removed. Three principles apply everywhere:

- **Least privilege.** Every person, account and service gets the minimum access needed for its task, and nothing more.
- **Need to know.** Personal data is accessed only when a specific job requires it, never for convenience or curiosity.
- **Default deny.** Access that is not explicitly granted is refused, in the product and in the infrastructure.

2. Roles and what they may access

Role	Access granted	Enforced by
Seller (organisation owner)	Their own organisation's shows, trays, items, buyer identifiers, label PDFs, settings, billing and marketplace connections.	Every API request is scoped to the org_id claim in the caller's token; cross-organisation reads and writes are impossible by construction.
Packer sub-account	Scanning and packing endpoints for their organisation only. No settings, billing, integrations, exports or account management.	Separate org_role claim checked against an explicit allow-list of endpoints; everything not listed is denied. Seats are capped and revocable by the owner.
Scan2Tray staff administrator	Customer support and operations views across organisations, for support, billing and abuse handling.	Separate admin claim issued only to named staff; admin actions are logged with actor, target and timestamp.
Partner administrator	Read-only support views limited to the customers that partner referred.	Partner claim plus a server-side scope filter applied to every allow-listed endpoint; no access outside the partner's own customers.
Engineer / infrastructure	Production servers, deployment platform and database for operating the service.	Per-device SSH keys over a private overlay network; key-only SSH with password login disabled; deployment platform account with MFA; production credentials issued per person and never shared.
Marketplace integrations	Only the API scopes required to read orders and identify the authorised shop.	OAuth scopes requested are the minimum for the feature; tokens are stored encrypted and used only server-side; sellers can revoke at any time.

3. Technical safeguards

- Authentication uses short-lived signed tokens with rotating refresh tokens; passwords are stored as salted BCrypt hashes; sign-in and device-pairing endpoints are rate-limited per IP.

- Personal data (buyer identifiers, names on slips, addresses in uploaded labels) is exposed only through authenticated, organisation-scoped endpoints. Label PDFs are never served from a public path.
- Secrets and API keys are held as environment variables on the deployment platform, never in source control or on endpoints.
- Local development uses test credentials and a local database that contains no customer data.

4. Granting, reviewing and removing access

- Staff and contractor access is approved by the Director, recorded, and limited to the role's needs. Production access is granted only to those who operate the service.
- Access is reviewed whenever a role changes and at least annually; unused access is removed.
- When someone leaves, all of their access is removed on the same day and any shared secret they held is rotated.
- Sellers manage their own packer seats and marketplace connections from the application and can remove either instantly.

5. Monitoring

Authentication failures, authorisation denials, rate-limit triggers and all administrative actions are logged. Anomalies are investigated under the incident process in the Information Security Policy.