Scan2Tray

Operational Security Baseline

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 and Endpoint Security Standard.

1. Purpose

This baseline sets the minimum day-to-day security behaviours expected of everyone who works on Scan2Tray systems or has access to customer or marketplace data. It is deliberately short so that it is followed, and it is reviewed with the Information Security Policy at least annually.

2. Daily baseline

Area	Requirement
Screen locking	Devices lock automatically after no more than 5 minutes of inactivity and immediately when the lid is closed or the device is left. Unlock requires the account password or biometrics. Devices are locked manually before being left unattended, including at home.
Passwords	Unique passwords per service, generated and stored in a password manager; never reused, shared, written down or sent by message. Staff account passwords are at least 14 characters. Default and vendor passwords are changed before use. Passwords are rotated immediately if a device or service may have been compromised.
Multi-factor authentication	MFA is enabled on every account that can affect production or customer data where the provider supports it: source control (GitHub), hosting and deployment (Hetzner, Coolify), domain and DNS registrar, email, payment provider (Stripe), marketplace partner and developer accounts (including TikTok Shop Partner Center), and app store accounts. Authenticator-app or hardware-key factors are preferred over SMS.
Clear desk and clear screen	No customer, buyer or marketplace data is printed or kept on paper. Test label printouts are shredded or binned once used. Screens are positioned or locked so that customer data is not visible to others when working outside the office.
Access to production	Production servers are reached only over the private administration network with per-device SSH keys. Production credentials are never pasted into chat, tickets or documents. Local development uses test credentials and a local database that contains no customer data.
Email and messaging	Links and attachments in unexpected messages are not opened; requests to change bank details, share credentials or approve access are verified out-of-band. Suspected phishing is reported to the security owner.
Software and updates	Only software from trusted sources is installed. Operating-system and browser updates are applied automatically; other updates within 14 days of release.
Devices and removable media	Only company-managed devices meeting the Endpoint Security Standard are used for production access. Removable media is not used to move customer data.
Working away from the office	Public Wi-Fi is used only with the device's VPN/overlay network active. Devices are never left unattended in vehicles or public places.
Leavers and role changes	Access to every system is removed on the day a person leaves or changes role; shared secrets they held are rotated.

3. Customer-facing controls

The same principles are applied inside the product. Seller passwords are stored only as salted BCrypt hashes; sign-in uses short-lived tokens with rotating refresh tokens and per-IP rate limiting; password reset and email verification use single-use, time-limited links; and sellers can revoke a connected marketplace or a packer sub-account at any time.

4. Reporting

Anything that looks wrong — a lost device, a suspicious message, an unexpected login alert, a credential that may have leaked — is reported to the security owner immediately at hello@scan2tray.com and handled under the incident process in the Information Security Policy. Reporting early is never penalised.