Scan2Tray

Endpoint Security 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. Scope

This standard applies to every computer used by Scan2Tray staff or contractors to develop, deploy or administer Scan2Tray systems, or to access customer or marketplace data. Scan2Tray is a small team; endpoints are limited to a small number of macOS workstations and a Windows build machine used to produce desktop application releases.

Customer and marketplace data is held on the hosted platform and accessed through the web application or over the private administration network. It is not stored on endpoints as a matter of course.

2. Baseline requirements

Control	macOS	Windows
Malware protection	Apple XProtect signature-based scanning and XProtect Remediator, with Gatekeeper and notarisation enforcement enabled. Definitions update automatically through Apple's background security updates.	Microsoft Defender Antivirus with real-time protection, cloud-delivered protection and automatic definition updates enabled. Tamper protection on.
Full-disk encryption	FileVault enabled.	BitLocker enabled on the system drive.
Operating-system currency	A currently supported macOS release with automatic installation of security responses and system updates.	A currently supported Windows release with Windows Update automatic installation enabled.
Host firewall	macOS application firewall enabled.	Windows Defender Firewall enabled on all profiles.
System integrity	System Integrity Protection enabled; only App Store or notarised software installed.	Secure Boot enabled; software installed only from trusted publishers.
Access	Per-user accounts; screen lock after inactivity with password or biometric unlock; no shared accounts. Administrative rights limited to the device owner.	
Authentication to services	Multi-factor authentication on source control, hosting/deployment, domain, email, marketplace partner and payment provider accounts wherever the provider offers it. SSH access to production uses per-device keys only.	
Data handling	Production credentials and marketplace secrets are never stored in plain files on endpoints; local development uses separate test credentials and a local database with no customer data.	

3. Lost, stolen or compromised devices

- Report to the security owner immediately.
- Remote-lock or erase the device (Find My / Microsoft account) and rotate every credential and SSH key the device held; revoke its Tailscale node.

- Treat as a security incident under the Information Security Policy if any customer or marketplace data could have been exposed.

4. Verification

Endpoint compliance is checked by the security owner at least annually and whenever a device is added or replaced. Devices that do not meet this standard are not used to access production systems until brought into compliance.