



POLICY · INFRASTRUCTURE AND OPERATIONS

Endpoint Security Policy

Version 1 · Approved by Jacek Janczura · 18 October 2026

Taufolio · Jacek Janczura
Adama Mickiewicza 73, 01-625 Warszawa, Poland
EU VAT: PL5253008276 · support@taufolio.com

Contents

1. Objective

2. Scope

3. Policy statement

4. Definitions

5. Endpoint security guidelines

6. Document security classification

7. Non-compliance

8. Responsibilities

9. Schedule

10. Version history

1. Objective

This policy sets out how Taufolio prevents unauthorized access to its production systems and critical data through endpoints such as the laptops used by staff members. It also describes what must be done if an endpoint is lost, stolen or damaged.

2. Scope

This policy applies to all staff members who use an endpoint to access Taufolio production systems or critical data within the scope of Taufolio's information security management.

3. Policy statement

Securing endpoints is essential to the confidentiality, integrity and availability of customer data. To secure their endpoints, staff members must install firmware and software updates, run protection software on endpoints that can reach critical systems, enable full-disk encryption, use strong passwords stored in a password manager, use multi-factor authentication, enable automatic screen lock, report lost or damaged devices, follow the removable media guidelines, and cooperate with periodic reviews.

4. Definitions

- **Endpoint:** any device that connects to a network, including laptops, desktops, mobile phones and tablets, and any server.
- **Endpoint security:** the measures that protect Taufolio systems when they are accessed from such devices. Every device that can reach Taufolio systems is a potential entry point for threats.

5. Endpoint security guidelines

Staff members must take the following steps to secure the endpoints they use for their work.

- **Updates.** Staff members are responsible for installing critical firmware and operating system updates on the endpoints they use or own. Automatic operating system updates must be enabled. Any shared device must have an assigned owner.
- **Protection software.** Every endpoint with access to critical systems, such as production infrastructure, must run the operating system's built-in protection or an equivalent anti-malware tool, kept current.
- **Disk encryption.** Staff members must turn on full-disk encryption in the operating system, for example FileVault on macOS or BitLocker on Windows.
- **Passwords and password manager.** Staff members must use strong passwords, as set out in the Access Control Policy, and must store them in an approved password manager. Passwords must

never be written down or kept in plain-text files.

- **Multi-factor authentication.** MFA must be enabled on every account that gives access to production systems or customer data, including the accounts at the hosting, database, authentication, source code and email providers.
- **Screen lock.** Staff members must enable automatic screen lock after a short period of inactivity, no longer than 20 minutes, and should lock the screen whenever they leave the device, rather than relying on the timer alone.
- **Lost, stolen or damaged devices.** Staff members must report a lost, stolen or damaged device to the Information Security Officer immediately. The Information Security Officer will then revoke access to critical systems and data from that device, for example by ending sessions and rotating credentials, and will assess whether a security incident must be declared.
- **Removable media.** Staff members must follow the removable media rules in the Asset Management Procedure. Customer data and credentials must not be copied to removable media.
- **Verification.** Compliance with this policy is checked through periodic self-attestation, in which each staff member confirms disk encryption, automatic updates, screen lock, password manager and MFA. The Information Security Officer records the results, and verification is complemented by internal reviews and audits.

Endpoint security does not require Taufolio to collect, log or track personal activity such as websites visited or purchases, to view a device remotely, or to log keystrokes.

6. Document security classification

Public. This document is published in the Taufolio Trust Center. See the Data Classification Policy for the classification levels.

7. Non-compliance

Compliance with this policy is verified through periodic self-attestation, code review, provider audit logs, internal reviews and feedback to the policy owner. Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or of their contractual agreement. The action depends on the extent, intent and consequences of the violation.

8. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures, and for recording the results of the endpoint checks. Staff members are responsible for applying the relevant sections of this policy in their own work.

9. Schedule

This document is reviewed at least annually and whenever a significant change occurs in Taufolio's systems or organization.

End of Endpoint Security Policy. For the version history, see the next page.

10. Version history

Version	Change	Approved by	Date
1 (current)	Taufolio policy issued for the Taufolio service and published in the Taufolio Trust Center	Jacek Janczura, owner	18 October 2026