



PROCEDURE · INFRASTRUCTURE AND OPERATIONS

Asset Management Procedure

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. Asset management procedure

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

The objective of this procedure is to describe the steps Taufolio follows to maintain, handle and protect all of its information assets, in support of the Asset Management Policy.

2. Scope

This procedure applies to all staff members (employees and contractors) who use or have access to Taufolio's information assets and data.

3. Asset management procedure

3.1 Inventory of assets

- An up-to-date inventory of assets must be maintained at all times. The Information Security Officer keeps it in Taufolio's internal documentation.
- The inventory must cover at least:
 - endpoints (laptops and mobile devices) used to access Taufolio data;
 - cloud accounts and SaaS subscriptions, including hosting, database, authentication, payments, email, analytics, monitoring, source control and AI model providers;
 - domains and the DNS and certificates attached to them;
 - data stores, including the production database, file storage and backups;
 - cryptographic keys and secrets, recorded by name, purpose and location, never by value.
- Where a provider keeps its own list (for example the repositories in GitHub or the members of the hosting and database projects), the Information Security Officer may use that list as a source, and must record any asset that such lists do not cover.
- Each entry must record the asset owner and the asset classification, as defined in the Data Classification Policy. Asset owners are responsible for keeping their entries accurate.
- The Information Security Officer must verify the inventory when it is first created and at least once a year thereafter.

3.2 Managing infrastructure assets

- A new infrastructure asset, such as a new cloud service, database, domain or integration, must be added to the inventory before it is used with production data or customer data. A new subprocessor must also pass the review defined in the Vendor Management Policy.
- The Information Security Officer is responsible for classifying every infrastructure asset. The classification is based on the type of data the asset processes and its criticality to the service, following the Data Classification Policy.

- The security controls required by the classification must be recorded alongside the asset. Examples are enforced MFA, encryption at rest, Sensitive status for production environment variables, and restricted database access.
- Control status must be checked against the providers' own settings and audit logs (GitHub, Vercel, Supabase, Clerk) at least once a year, and after any significant change.
- A failed or missing control must be corrected promptly. A gap that remains open longer than the period set by the Information Security Officer must be recorded in the risk register (see the Risk Assessment and Management Policy).

3.3 Managing endpoint assets

- The list of all endpoint devices used to access Taufolio data is maintained in the inventory. Staff members may use their own devices or devices supplied by Taufolio.
- Every staff member must report each device they use to access Taufolio data to the Information Security Officer, and must report any change.
- The Information Security Officer must ask every staff member to confirm their devices and security status at least once a quarter.
- Staff members must follow these steps to keep their endpoints secure, in line with the Endpoint Security Policy:
 - install critical operating system, firmware and software updates promptly;
 - run anti-malware protection on every endpoint with access to critical data;
 - turn on full-disk encryption of the operating system (for example FileVault on macOS);
 - protect accounts and devices with strong passwords, using a password manager, as set out in the Access Control Policy;
 - enable automatic screen lock after a short period of inactivity, and not leave a device unattended and unlocked;
 - report a lost, stolen or damaged device to the Information Security Officer immediately, so that access to production systems and customer data from that device can be revoked;
 - follow the removable media rules in the Asset Management Policy and the Physical and Environmental Security Policy.
- Endpoints may be verified against these requirements through periodic reviews and confirmation by staff members.

3.4 Review of assets

The Information Security Officer must review the list of infrastructure assets and critical systems at least annually, and after any significant change, and must remove assets that are no longer used, together with their access and data.

4. Document security classification

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

5. Non-compliance

Compliance with this procedure is verified through the inventory reviews, provider audit logs, periodic internal reviews and feedback to the policy owner. Any staff member found to have violated this procedure 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.

6. Responsibilities

The Information Security Officer is responsible for approving and reviewing this procedure and the related policies, and for maintaining the asset inventory. Staff members are responsible for applying the relevant sections of this procedure in their own work.

7. Schedule

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

End of Asset Management Procedure. For the version history, see the next page.

8. Version history

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