



POLICY · INFRASTRUCTURE AND OPERATIONS

Asset Management 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. Asset management

5. Data classification

6. Management of removable media

7. Disposal of media

8. Document security classification

9. Non-compliance

10. Responsibilities

11. Schedule

12. Version history

1. Objective

The objective of this policy is to provide a framework that ensures Taufolio's information assets and data are protected and handled appropriately throughout their life, from acquisition to disposal.

2. Scope

This policy applies to all assets used across the processes and operations within the scope of Taufolio's information security program, and to every staff member (employees and contractors) who uses or has access to them.

3. Policy statement

All Taufolio assets must be identified, owned, classified and appropriately protected, and information must be handled and exchanged in line with its classification. This prevents unauthorized disclosure, modification, removal or destruction of assets and interruption to the service Taufolio provides to its users.

4. Asset management

4.1 Types of assets

The following are the types of assets that must be treated as information assets:

- **Infrastructure assets:** databases and file storage, hosting and serverless compute, content delivery and firewall services, and the source code repository.
- **Software assets:** the application code, third-party libraries, system software, development tools and utility software.
- **Cloud accounts and SaaS subscriptions:** accounts and subscriptions with providers such as Vercel, Supabase, Clerk, Stripe, Resend, PostHog, Sentry, GitHub and the AI model providers.
- **Domains and certificates:** registered domain names, DNS records and the certificates that protect them.
- **Keys and secrets:** encryption keys, the master key for customer credentials, API keys, service tokens and other secrets.
- **Physical assets:** laptops, mobile devices and other equipment used by staff members, and any removable media.
- **Service assets:** computing and communication services, and third-party suppliers on which Taufolio depends.
- **People assets:** staff members, including employees and contractors.

- **Documents:** contracts, agreements, non-disclosure agreements, system documentation, policies and procedures, continuity and recovery plans, audit trails and archived information.

4.2 Responsibility for assets

- Every information asset must have an asset owner assigned, responsible for its production, development, maintenance, use and security. Where needed, the owner may nominate a custodian who is a different person.
- The asset owner is responsible for:
 - ensuring that the asset and the information processing facilities associated with it are appropriately classified;
 - defining and maintaining the security of the asset, and helping the Information Security Officer periodically review access restrictions and classifications, taking the Access Control Policy into account.
- Because information is important and pervasive at Taufolio, every user has a role in protecting the information entrusted to them. Every staff member who may come into contact with non-public information must read and understand this policy and the Asset Management Procedure.

4.3 Inventory of assets

- An up-to-date inventory of assets must be maintained at all times, by the Information Security Officer, in Taufolio's internal documentation.
- The owner of each asset type is responsible for keeping its entries current. Owners may differ by type of asset.
- At a minimum, each entry must include an asset identifier, an asset classification and an asset owner.

4.4 Acceptable use of assets

- The acceptable use of assets must be clearly defined.
- All staff members who use or interface with Taufolio assets must acknowledge that they know and accept the rules for acceptable use.

4.5 Return of assets

When a staff member leaves Taufolio or their contract ends, they must return or hand over all information assets under their control, including devices, credentials, keys and data, and their access must be removed.

5. Data classification

Information assets must be classified according to their business value, legal requirements, sensitivity and criticality. Handling an asset appropriately requires understanding the type of data it processes, in

particular whether it holds customer brokerage credentials or personal data. See the Data Classification Policy for the classification levels and handling rules.

6. Management of removable media

Using removable media such as USB sticks or external hard drives to transfer data is prohibited. Any such use is a violation of this policy. Data must be moved only through approved, access-controlled services.

7. Disposal of media

Disposal of media, both electronic and physical, must protect data from exposure to unauthorized people. When media is no longer required, it must be disposed of securely and in line with documented guidelines. The level of destruction depends on the data stored on the media and its classification. Devices that held Taufolio data must be wiped or physically destroyed before they are reused, sold or discarded. See the Data Classification Policy for the applicable levels.

8. Document security classification

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

9. Non-compliance

Compliance with this policy is verified through the asset inventory reviews, provider audit logs, periodic 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.

10. Responsibilities

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

11. Schedule

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

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

12. 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