



POLICY · DATA PROTECTION AND PRIVACY

Data Classification 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. Data classification definitions

5. Labeling of information

6. Document security classification

7. Non-compliance

8. Responsibilities

9. Schedule

10. Version history

1. Objective

This policy provides a way to categorize all data processed by Taufolio staff, software and systems. It establishes a framework for classifying data by its sensitivity, value and criticality, so that anyone handling data can map it to the level of protection and access it needs. This clarity ensures that the data that matters most, above all the credentials customers entrust to Taufolio, is secured accordingly.

2. Scope

This policy applies to all data handled, managed, stored or transmitted by Taufolio and its staff members (employees and contractors), in any form and on any system, including the production application, the database and file storage, endpoints, and the third-party services that process data on Taufolio's behalf. The Information Security Officer and the owner of each information asset assign the appropriate classification when an asset is created or changes.

3. Policy statement

Every staff member is responsible for reviewing, following and handling data according to the classification levels defined below. When a data element is hard to classify, or the risk and the right handling are unclear, the staff member must ask the Information Security Officer before proceeding. Data without a recorded classification must be treated as Confidential until classified. A collection of data takes the level of its most sensitive element.

4. Data classification definitions

Taufolio data is classified at one of four levels, from lowest to highest sensitivity.

4.1 Public

Information that may be shared with anyone and whose disclosure causes no harm to Taufolio, its users or its partners. It needs no special safeguarding against disclosure, only protection of its integrity.

Examples: the Taufolio website, blog and academy content, published legal documents and the Trust Center, pricing, press material, and public market information presented in reports.

4.2 Internal

Information used for Taufolio's day-to-day operation that is not meant for outsiders. It is available to all staff members and may be shared externally on request when there is a reason to do so.

Examples: internal procedures and runbooks, the asset inventory, non-public policy drafts, internal documentation and the issue tracker content that holds no personal data.

4.3 Confidential

Information whose unauthorized access or disclosure could harm users, Taufolio or its partners, cause a breach of law or contract, or create a security incident. Access is limited to authorized staff members on a need-to-know basis. Confidential information must be protected when stored, processed and transmitted.

This level includes all personal data and customer data:

- portfolio holdings, watchlists, transactions, balances and dividends, whether entered, uploaded or imported from a brokerage;
- account and profile data (name, email address, authentication identifiers), billing status and invoices, support tickets and bug reports, and the screenshots and files attached to them;
- user-written content such as journal entries, notes and assistant conversations;
- security and audit logs, and unpublished source code;
- business information such as contracts, financial records and internal roadmaps.

4.4 Restricted

The highest level. Information whose compromise could directly damage users' financial accounts or the integrity of the whole service. Access is limited to the minimum number of systems and persons, is never granted for convenience, and where possible is limited to automated processes without any human access.

This level includes:

- **customer brokerage credentials:** OAuth client identifiers and client secrets, access and refresh tokens, API keys and any provider-issued user secret;
- the master encryption key for customer credentials, and every other cryptographic key, signing secret and server-side database secret key;
- production secrets and tokens of Taufolio's providers (hosting, database, authentication, payments, email, AI model providers);
- administrative credentials and recovery codes of staff accounts.

Restricted information must be:

- encrypted by the application before storage where it belongs to customers, and stored only in a purpose-built secret store or a dedicated server-only table, never in source code, documents, chat messages, logs, error reports, analytics or AI prompts;
- readable only in memory, by the server process that needs it, and never returned to a browser or displayed to staff;
- transmitted only over TLS;
- rotated on suspected compromise and whenever a person with access leaves Taufolio, with any incident handled under the Incident Management Policy.

4.5 Handling summary

Level	Who may access	Storage and transfer	Disposal
Public	Anyone	No special requirement	None required
Internal	All staff members	Company-managed accounts and devices	Delete when obsolete
Confidential	Authorized staff, need-to-know	Encrypted at rest and in transit, access logged where the provider supports it	Delete under the Data Retention and Deletion Policy
Restricted	Server processes; the Information Security Officer for keys only	Application-layer encryption or a secret store, TLS only, never in logs	Immediate hard deletion on revocation; keys destroyed after rotation

5. Labeling of information

The asset owner must label information according to this policy where the format permits, for example in the asset inventory, in document headers, in database table and column documentation, and in repository folders. Most of Taufolio's critical information is electronic, so labeling is done mainly through tagging in the asset inventory and through the technical controls attached to each store, such as Row Level Security and secret stores. Information that has no label is treated as described in section 3.

6. Document security classification

Public. This document is published in the Taufolio Trust Center.

7. Non-compliance

Compliance with this policy is verified through code review, automated tests, 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.

8. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures, and for resolving classification questions. 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, data or organization.

End of Data Classification 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