



POLICY · THIRD PARTIES AND COMPLIANCE

Compliance 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. Compliance policy

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

This policy establishes guidelines for managing the regulatory, legal and contractual compliance requirements that apply to Taufolio's systems. It covers the GDPR and the standards Taufolio's controls are designed to, namely ISO/IEC 27001:2022 Annex A and the AICPA SOC 2 Trust Services Criteria (Security, Availability and Confidentiality).

Taufolio is GDPR compliant. It is "ISO 27001 ready" and "SOC 2 ready"; it holds no certification, has not been audited against either framework, and no attestation report exists.

2. Scope

This policy applies to all processes and operations of Taufolio within the scope of the Information Security Management System (ISMS), as defined in the Information Security Policy.

3. Policy statement

Taufolio's ISMS must be established and operated with due consideration for statutory, regulatory and contractual obligations and any specific security requirements, including the contractual and technical requirements of brokerage providers that grant Taufolio read-only access to user accounts.

4. Compliance policy

4.1 Identification of applicable legislation and compliance requirements

All relevant statutory, regulatory and contractual requirements must be explicitly defined and documented for Taufolio's information systems, and Taufolio's policies and procedures must follow the applicable laws. Documentation of requirements is mandatory for the ISO/IEC 27001 control set Taufolio designs to. For other standards, compliance with the applicable requirements must be ensured, and explicit documentation is not required.

4.2 Intellectual property rights

Taufolio must comply with the terms and license requirements of copyrighted software, third-party content, user intellectual property and any other proprietary information used in the organization, including the terms of use of the services and data sources it integrates.

4.2.1 Protection of organizational records

Records related to information security must be protected from loss, destruction and falsification in accordance with statutory, regulatory, contractual and business requirements.

4.2.2 Data protection and privacy of personal information

Data protection and privacy must be ensured as required by the relevant legislation (including the GDPR), regulations and any contractual clauses. See the Data Protection Policy for guidance on protecting personal information.

4.2.3 Prevention of misuse of information processing facilities

Information processing facilities must be used in accordance with this policy, the Acceptable Usage Policy and the Code of Business Conduct Policy. Disciplinary action must be taken for violations.

4.2.4 Compliance with security policies, standards and technical compliance

The Information Security Officer must ensure that all security procedures within their area of responsibility are carried out correctly, so that Taufolio complies with its security policies and standards.

4.2.5 Information systems audit considerations

- Taufolio must carry out periodic audits by competent, independent parties to confirm compliance with security policies, procedures, standards and guidelines. Formal procedures must be defined for planning and reporting audits and for addressing findings with prompt and accurate remedial action.
- Audit requirements and activities involving checks on operational systems must be carefully planned and agreed, to minimize the risk of disruption to the business and to users.
- Access to information systems audit tools must be protected to prevent misuse or compromise.
- Auditors must not be given access to brokerage credentials. Audit evidence must be produced from configuration, access records and test results, never from decrypted customer secrets.

5. Document security classification

Public. See the Data Classification Policy for the full set of classification levels.

6. Non-compliance

Compliance with this policy is verified through various methods, including provider audit logs, periodic reviews, audits and feedback to the policy owner. Any staff member found to violate this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action depends on the extent, intent and repercussions of the violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures. Staff members are responsible for implementing the relevant sections of the policy in their area of work.

8. Schedule

This document must be reviewed annually and whenever significant changes occur in the organization.

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

9. 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