



PROCEDURE · THIRD PARTIES AND COMPLIANCE

Compliance 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. Compliance with legal requirements

4. Safeguarding organizational records

5. Independent reviews of compliance with security policies and standards

6. Technical compliance checking

7. Intellectual property rights

8. Information systems audit

9. Corrective and preventive actions

10. Document security classification

11. Non-compliance

12. Responsibilities

13. Schedule

14. Version history

1. Objective

This procedure establishes the methods by which regulatory and legal compliance requirements are managed for the systems within the scope of Taufolio's Information Security Management System (ISMS).

2. Scope

This procedure applies to all processes and operations at Taufolio within the scope of the ISMS, as defined in the Information Security Policy. It implements the Compliance Policy.

3. Compliance with legal requirements

3.1 Identification of applicable legislation

- The Information Security Officer, with legal advisers and engineering input as needed, must identify legislation that affects Taufolio's policies and procedures, including the GDPR and the requirements of brokerage providers that grant read-only access.
- The Information Security Officer must record the applicable legislation in Taufolio's internal ISMS documentation and keep it current.
- Advice on statutory, regulatory and contractual requirements must be sought from engineering and, where needed, external legal counsel.
- The Information Security Officer must ensure that the controls needed for compliance are implemented.
- Compliance must be reviewed periodically by engineering together with the Information Security Officer.

3.2 Data protection and privacy of personal information

- Data protection and privacy must be ensured as required by the identified legislation, regulations and contractual clauses.
- The identified requirements must be communicated to everyone involved in processing personal information.
- The Information Security Officer must give staff members the guidance they need on their responsibilities and the procedures to follow.
- Access to personal information must be on a need-to-know basis. Brokerage credentials are never accessible to staff; they are encrypted by the application and decrypted only in memory by the server process that calls the broker, as set out in the Encryption Policy.

4. Safeguarding organizational records

All organizational records must be managed in accordance with the Data Classification Policy.

4.1 Prevention of misuse of information processing facilities

Information processing facilities must be used in accordance with the Acceptable Usage Policy.

5. Independent reviews of compliance with security policies and standards

- Compliance with the following policies and procedures must be monitored continuously:
 - Human Resources Security
 - Asset Management
 - Physical and Environmental Security
 - Operations Security
 - System Acquisition and Development
 - Vendor Management
 - Access Control
 - Network Security
 - Incident Management
 - Compliance
- The Information Security Officer must ensure that all security procedures are tracked as defined, using the access register, the asset inventory and provider audit logs (GitHub, Vercel, Supabase, Clerk).
- The Information Security Officer is responsible for educating staff members on the security policies and procedures.
- Each staff member responsible for an area must regularly review compliance in that area. If non-compliance is found, they must:
 - determine its causes;
 - evaluate the need for action to prevent recurrence;
 - determine and implement appropriate corrective action;
 - inform the Information Security Officer where required.
- The Information Security Officer must review all areas once a year to confirm compliance with security policies and procedures.

6. Technical compliance checking

One annual technical assessment and review must be performed by a competent third party together with engineering, to identify potential vulnerabilities in networks and production systems. The findings must be reported to the Information Security Officer and tracked to closure as set out in section 9.

7. Intellectual property rights

Engineering and the Information Security Officer must ensure that all third-party software and services are appropriately licensed and do not violate copyright or other intellectual property rights.

8. Information systems audit

8.1 Preparing and conducting audits

Taufolio relies on continuous controls such as provider audit logs, repository protections and automated checks, and in addition an annual audit of the control environment must be performed to confirm compliance is maintained. The audit must consider:

- completeness of the inventory of assets and systems;
- adherence to procedure timelines;
- review of the list of vendors and subprocessors;
- review of information security risks;
- review of the protection of customer brokerage credentials against the Encryption Policy.

The audit may be performed by the Information Security Officer or by an independent party. Results must be recorded and reviewed by the owner at least annually.

8.2 Audit reports, findings and non-conformance closure

- Auditors must record non-conformances, observations and suggestions in the internal audit report.
- Corrective actions must be documented in a corrective and preventive action (CAPA) register.
- The internal audit report and the CAPA register must be presented to the owner for review.
- The responsible person must start corrective and preventive action on each non-conformance and close it within the committed time.
- At the end of that time, the Information Security Officer must verify that the non-conformance is closed.

9. Corrective and preventive actions

The corrective and preventive action process must be started whenever a condition warrants investigation to determine whether corrective or preventive action is needed. This process supports the ISO/IEC 27001:2022 Annex A design of Taufolio's controls.

9.1 Corrective actions

Corrective action must be documented in the CAPA register whenever a non-conformance is raised in an internal audit. It must also be initiated as a result of, but not limited to:

- non-conformances identified in internal or external audits and assessments;
- action items from management reviews of information security effectiveness;
- reported security incidents;
- reported deviations in the provision of services;
- security weaknesses reported by staff members or users;
- violations of security policy and security objectives.

9.2 Preventive actions

- The Information Security Officer must keep a summary of corrective and preventive actions taken, with their details, in the same register.
- Preventive action must be determined from analysis of appropriate data to detect trends and identify causes that may lead to future non-conformances.
- The Information Security Officer must verify the effectiveness of the corrective and preventive action taken.
- The results of corrective and preventive actions must be reviewed by the owner at least annually.

10. Document security classification

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

11. Non-compliance

Compliance with this procedure 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 procedure 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.

12. Responsibilities

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

13. Schedule

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

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

14. 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