



POLICY · GOVERNANCE

Information Security 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. Information security requirements

5. Information security objectives

6. Segregation of duties

7. Contact with special interest groups

8. Contact with authorities

9. Information security in project management

10. Reporting of security incidents

11. Maintenance of policy

12. Supporting policies

13. Document security classification

14. Non-compliance

15. Responsibilities

16. Schedule

17. Version history

1. Objective

Taufolio produces AI-assisted equity research and offers a portfolio tracker. To do so, Taufolio and its subprocessors hold personal data, portfolio data and, where a user connects a brokerage account, the credentials that allow Taufolio to read it. Users place a great deal of trust in Taufolio to create, store, share and transmit that data securely. Loss of data or service through unauthorized access, intrusion, theft, disaster or cyber-attack would damage that trust and Taufolio's reputation.

This policy defines the direction, principles and basic rules for information security management at Taufolio. It states management's commitment to protect confidentiality, maintain integrity and ensure availability of information assets, and to respond to and recover from security incidents.

Information security safeguards three objectives:

- **Confidentiality:** data and information assets are confined to people authorized to access them and are not disclosed to others.
- **Integrity:** data is kept intact, complete and accurate, and information systems remain operational.
- **Availability:** information and systems are at the disposal of authorized users when needed.

2. Scope

This policy applies to:

- all staff members (employees and contractors) who have access to Taufolio's or its users' information;
- all vendors and third parties who have access to Taufolio's information processing systems and the data in them;
- all stakeholders and interested parties relevant to Taufolio's operations;
- all digital and non-digital assets involved in the creation, storage, transmission and disposal of information.

3. Policy statement

Taufolio must establish, implement and maintain an Information Security Management System (ISMS). The ISMS is the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain and improve information security. It includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

The ISMS must protect confidentiality, maintain integrity and ensure availability of information assets, and must enable Taufolio to respond to and recover from incidents.

When planning the ISMS, Taufolio must consider internal and external issues and the requirements of interested parties, and determine the risks and opportunities that could affect the delivery of its products

and services. Management must provide the resources the ISMS needs to achieve its intended outcomes.

Taufolio's controls are designed to the ISO/IEC 27001:2022 Annex A and to the AICPA SOC 2 Trust Services Criteria (Security, Availability and Confidentiality). Taufolio is GDPR compliant. Taufolio is "ISO 27001 ready" and "SOC 2 ready"; it holds no certification and has not been audited against either framework, and no attestation report exists.

4. Information security requirements

Information and supporting technology, including hardware and software systems, are critical business assets. Their confidentiality, integrity and availability are essential to legal compliance, user trust and the continuity of the business.

Organizations and their systems face threats from many sources, including external hacking and intrusion, computer-assisted fraud, espionage, sabotage, vandalism and natural disaster. Dependence on information systems and services makes these threats more serious.

Designing and implementing security controls requires careful planning. Management policies and administrative controls must supplement the technical controls that protect data. Information security needs the participation of every staff member and may also involve suppliers, service providers, users and external specialists.

Customer credentials for brokerage connections are the most sensitive data Taufolio holds. They must be protected as set out in the Encryption Policy, the Access Control Policy and the Data Classification Policy: encrypted by the application before they reach the database, never logged or displayed, limited to read-only broker scopes, and deleted on disconnect or account deletion.

5. Information security objectives

The objectives of this policy are:

- to create a coherent system for managing information security that is aligned with Taufolio's business strategy;
- to protect the information that is important to Taufolio and its users;
- to reduce the risk related to the use of technology and the outsourcing of technology to subprocessors;
- to ensure that all information assets are accounted for and protected from damage, alteration, loss and unauthorized use or access;
- to ensure that information and information systems are available only to authorized users;
- to give users the means to exercise their rights to access, correct and erase personal data about them;
- to ensure that personal data is processed only for the purposes for which it was collected and as documented in Taufolio's privacy information;

- to comply with all regulatory and statutory requirements for information collection, storage, processing, transmission and disclosure;
- to set aside resources to establish, implement, operate, monitor, review and maintain security safeguards;
- to make staff members aware of, and able to meet, their security responsibilities;
- to maintain detailed security guidelines and ensure compliance with them;
- to review these objectives periodically and drive continuous improvement.

6. Segregation of duties

Segregation of duties reduces the risk of accidental or deliberate misuse of Taufolio's assets. When responsibilities are assigned, conflicting duties and areas of responsibility must be separated to reduce opportunities for unauthorized or unintentional modification or misuse of assets. Every individual must access, modify or use assets only with proper authorization or detection, and the possibility of collusion must be considered when controls are designed. Where separation is not possible in a small team, compensating controls such as provider audit logs, code review and owner oversight must be applied, as described in the Organization of Information Security Policy.

7. Contact with special interest groups

The Information Security Officer must seek specialist advice when required, for example from a security consultant engaged per assignment, from non-profit security organizations and from vendor security advisories, after appropriate validation of the source.

8. Contact with authorities

Taufolio must maintain appropriate contact with law enforcement, regulatory bodies (including the data protection supervisory authority) and emergency services, so that help is accessible during a crisis.

9. Information security in project management

Information security must be integrated into how Taufolio plans and delivers work, so that security risks are identified and addressed as part of every project, whatever its character. For software changes this is done through code review, automated checks and the secure development practices in the System Acquisition and Development Policy.

10. Reporting of security incidents

Any person who witnesses or suspects an information security incident must report it immediately to the Information Security Officer by email to support@taufolio.com, with "Security incident" in the subject. Users may use the in-app "Report a problem" form. Reports are handled under the Incident Management Policy.

11. Maintenance of policy

- Compliance with this policy and the supporting policies must be reviewed yearly, and exceptions found must be addressed immediately and appropriately.
- This policy must be reviewed annually, and on need when a major change occurs in the organization or its environment.
- This policy must be reviewed and revised whenever a major security risk or incident is identified.

12. Supporting policies

At a minimum, the following documents support this policy.

12.1 Human Resources Security Policy

Ensures that staff members understand their responsibilities and are suitable for the roles for which they are considered.

12.2 Risk Management Procedure

Provides guidelines for understanding and managing the risks that may affect information security.

12.3 Access Control Policy

Limits access to information and information processing facilities, ensures authorized user access and prevents unauthorized access to systems and services, makes users accountable for safeguarding their authentication information, and supports segregation of duties.

12.4 Asset Management Policy

Identifies Taufolio's assets and defines protection responsibilities, ensures information receives a level of protection that matches its importance, and prevents unauthorized disclosure, modification, removal or destruction of information stored on media.

12.5 Operations Security Policy

Ensures the protection of information through the daily operations that deliver Taufolio's services.

12.6 Acceptable Usage Policy

Ensures staff members know how assets may be used and follow formal cybersecurity guidelines, and that information is protected when accessed, processed or stored while working remotely.

12.7 Compliance Policy

Ensures Taufolio meets its legal and regulatory requirements.

12.8 System Acquisition and Development Policy

Ensures information security is an integral part of information systems across their entire lifecycle, including systems that provide services over public networks.

12.9 Physical and Environmental Security Policy

Prevents unauthorized physical access, damage and interference to Taufolio's information and information processing facilities.

12.10 Business Continuity Management Policy

Embeds business continuity in Taufolio's operations.

12.11 Vendor Management Policy

Protects Taufolio's assets that are accessible to or provided by third-party suppliers and subprocessors.

12.12 Incident Management Policy

Governs the management of incidents that may compromise the confidentiality, integrity or availability of data and services.

13. Document security classification

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

14. 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.

15. Responsibilities

- The Information Security Officer has ultimate authority over this policy and approves and authorizes all changes to it.
- The Information Security Officer has executive authority over information security and issues all ISMS documentation.
- The Information Security Officer is responsible for developing and maintaining all ISMS documentation.
- The Information Security Officer must schedule periodic internal audits, carried out by Taufolio itself or by external consultants.
- The Information Security Officer, as Data Protection contact, is responsible for a privacy program that defines, develops, maintains and implements policies and processes for consistent, effective privacy practices, minimizes risk, and ensures the confidentiality of personal data in every medium.

The Information Security Officer role is held by Jacek Janczura, the owner of Taufolio.

16. Schedule

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

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

17. 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