



POLICY · GOVERNANCE

Organization of 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. Organization of information security

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

This document defines the governance framework of Taufolio's Information Security Management System (ISMS). It identifies the security organizational structure and assigns information security roles, responsibilities and authorities so that duties are properly separated. The policy exists to initiate and control the implementation of information security within the organization.

2. Scope

This policy applies to all processes and operations at Taufolio that fall within the scope of the ISMS, as defined in the Information Security Policy.

3. Policy statement

Responsibilities for information security at Taufolio must be clearly defined through role descriptions and task delegation. The Information Security Officer approves the information security policy and standards. Responsibilities include identifying information assets, classifying them, implementing controls and reviewing user access privileges. Segregation of duties and appropriate contact with authorities and special interest groups are required. Information security must be integrated into project management, and precautions for mobile devices and remote work are set out below.

4. Organization of information security

4.1 Information security roles and responsibilities

Taufolio is a small team. Jacek Janczura, the owner, holds the roles of Information Security Officer, Data Protection contact and approver of every policy. Other staff members hold the responsibilities allocated to them in writing.

- All information security responsibilities for the protection of Taufolio's sensitive information, information systems and information processing facilities must be clearly defined through role descriptions, work allocation and task delegation.
- The Information Security Officer must approve the information security policy.
- The Information Security Officer must approve standards, procedures, templates and guidelines.
- Defined responsibilities must be formally allocated and accepted across the organization. They include:
 - identifying information assets and the security processes associated with each asset;
 - defining and documenting asset ownership, level of responsibility and authorization levels, in the asset inventory kept by the Information Security Officer;

- classifying, labeling and handling information assets in accordance with the Data Classification Policy;
- identifying and implementing the controls needed to protect assets adequately, including encryption of customer brokerage credentials as set out in the Encryption Policy;
- reviewing and approving user access privileges in accordance with the Access Control Policy and Procedure, using the access register and the audit logs of GitHub, Vercel, Supabase and Clerk.

4.2 Segregation of duties

- Segregation of duties must be considered before assigning roles, to reduce opportunities for deliberate or accidental misuse of infrastructure or software. For example, the ability to initiate, authorize, execute and verify a request should be split so that no one person completes the entire request.
- Where segregation is not possible, compensating controls must be applied to detect misuse of access rights: activity monitoring, provider audit trails, review of changes in the private GitHub repository, and management supervision.
- When primary personnel are unavailable (illness, vacation or leave) and another person with a different role fills in, appropriate segregation or compensating controls must be considered.
- No individual role may combine unrestricted access to production systems with the ability to remove the audit trail of that access.

4.3 Contact with authorities

Appropriate contacts must be established and kept current with law enforcement authorities, regulatory bodies (including the data protection supervisory authority), subprocessors and software and hardware vendors.

4.4 Contact with special interest groups

The objective is to keep appropriate contact with special interest groups and authorized security forums, to receive and share updates on new vulnerabilities, threats, regulations and risks relevant to Taufolio's business.

The Information Security Officer must maintain these contacts in the interest of Taufolio's security posture and should consider:

- **Security forums**, which enhance the security of communications and infrastructure through collaboration, issue guidelines and advisories, and share information on the latest changes.
- **Security advisories**, which provide objective, timely and comprehensive information on threats and vulnerabilities, for example vendor and public advisory feeds and GitHub security alerts.
- **Application vendors and suppliers**, with whom contact must be kept so that the latest threats and vulnerabilities in the software Taufolio uses are addressed.
- **Other institutions** that can help solve security issues.

The purpose of these contacts is to:

- receive updates on new vulnerabilities, threats and regulations;
- improve knowledge and keep up to date with relevant security information;
- keep the understanding of the security environment current and complete;
- receive early warnings of alerts, advisories and patches for attacks and vulnerabilities;
- gain access to specialist security advice;
- share and exchange information about new technologies, products, threats and vulnerabilities.

4.5 Information security in project management

- Information security must be integrated into Taufolio's project management methods so that security risks are identified and addressed as part of projects.
- Information security implications must be considered regularly in all projects, including every new integration with a brokerage provider, which requires a review of the scopes requested (read-only only) and of how credentials are stored.

4.6 Mobile devices and remote work

4.6.1 Mobile devices

- When traveling (cars, hotels, conferences, meeting rooms, public places), staff members must take reasonable precautions to protect laptops from damage, theft and eavesdropping. An unattended laptop must be locked or shut down, concealed where possible, and never accessible without password protection.
- The loss of a laptop or mobile device that has access to Taufolio systems must be reported immediately to the Information Security Officer, so that sessions and credentials can be revoked.
- Staff members must not make changes that circumvent the security mechanisms of their device. Examples of unacceptable manipulation include setting up unauthorized network connections, switching off endpoint protection, and misusing privileges granted for business functions. Costs caused by such manipulation may be charged to the person responsible, in addition to disciplinary measures.
- Users are responsible for the confidentiality, integrity and availability of the information on their mobile computing devices.
- The Information Security Officer must ensure that every endpoint with access to production infrastructure has endpoint protection installed and full-disk encryption enabled, as set out in the Endpoint Security Policy.

4.6.2 Remote work

- Staff members must take all necessary precautions to secure information and equipment at home, prevent unauthorized access to any system or information, and comply with the Acceptable Usage

Policy.

- Taufolio's equipment must be protected against damage and unauthorized use. Staff members must designate a safe workspace, and safeguards must protect records from unauthorized disclosure or damage.
- Authority and access rights must be revoked and equipment returned when remote work ends or when the staff member leaves Taufolio.

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 Organization of Information Security 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