



POLICY · INFRASTRUCTURE AND OPERATIONS

Communications and Network 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. Communications and network security

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

Taufolio must take adequate precautions and design appropriate controls to prevent misuse of its information assets and information processing facilities. To this end Taufolio establishes communication and network security rules, protects information in networks and supporting infrastructure, keeps information in transfer secure, and detects unauthorized information processing.

2. Scope

This policy applies to all processes and operations within the scope of Taufolio's information security management, including the public website and application, the connections between Taufolio's servers and its subprocessors, brokerage providers and database, and electronic communication used by staff members.

3. Policy statement

Taufolio is committed to providing a dependable, secure service to its users. It is therefore essential to manage and control networks so that they are protected from threats and the security of the systems and applications that use them is maintained. Taufolio has no office network and no self-managed servers. Its network perimeter is the network of its hosting provider, and the controls in this policy apply to that perimeter and to all connections made by Taufolio's systems and staff.

4. Communications and network security

4.1 Network security management

4.1.1 Network controls

- Networks and network services must be managed and controlled to protect against threats and to maintain the security of the systems and applications that use them, including information in transit.
- Internet-facing systems must be protected by a firewall, limited connectivity and encryption. Taufolio uses the edge network and firewall of its hosting provider (Vercel) for this purpose. Where available, intrusion detection and prevention and attack-mitigation features of the providers must be enabled.
- Every connection to Taufolio's public properties must use HTTPS with TLS 1.2 or higher, and HTTP Strict Transport Security (HSTS) is enabled on taufolio.com.
- The database must not be publicly accessible: no anonymous access path may exist, and direct connections must be restricted to the application and to named administrators. Connections to the database must use SSL, and this must be enforced.
- Any system deployed on the internet must go through a vulnerability check before release and at least once a year afterwards.

- Network and firewall configuration may only be changed by trained and authorized staff, and every change must follow the Operations Security Procedure.
- Every endpoint that connects to Taufolio's infrastructure must meet the baseline set out in the Endpoint Security Policy.

4.1.2 Information transfer

- Information transfer rules are set out in the Data Classification Policy and the Asset Management Procedure, and staff members must be made aware of them.
- Acceptable use standards must define the appropriate use of communication facilities.
- Appropriate anti-malware controls must be in place to detect and prevent malware that could be transmitted through electronic communication.
- Staff members must treat all correspondence sent from Taufolio systems as confidential.
- To prevent loss, modification, destruction or misuse of information, the exchange of critical information and software with third parties must be protected and controlled. Data sent to subprocessors and brokerage providers must travel only over TLS.
- Web filtering that restricts access to harmful websites should be used where it is practical.

4.1.3 Electronic messaging

- Information in electronic messaging, such as email and chat, must be protected from unauthorized access, modification and denial of service.
- Personal email accounts must not be used for Taufolio business unless authorized.
- Forwarding of Taufolio mailboxes to external accounts must comply with the Data Classification Policy.
- Customer credentials, access tokens and other secrets must never be sent by email or chat.

4.1.4 Confidentiality and non-disclosure agreements

- Confidentiality or non-disclosure agreements that reflect Taufolio's need to protect information must be identified and maintained with third parties, based on the criticality of the information involved.
- These requirements must be reviewed at least once a year and whenever the business environment, legal requirements or contractual obligations change.
- Such agreements must comply with the laws and regulations that apply to them.
- Staff members and contract partners must sign and comply with the confidentiality agreement that Taufolio maintains, where applicable.

5. Document security classification

Public. This document is published in the Taufolio Trust Center. See the Data Classification Policy for the classification levels.

6. 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.

7. Responsibilities

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

8. Schedule

This document is reviewed at least annually and whenever a significant change occurs in Taufolio's systems or organization.

End of Communications and Network 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