



PROCEDURE · INFRASTRUCTURE AND OPERATIONS

Network Security 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. Network security management

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

Network security reduces information security risk and protects Taufolio against unintended disclosure of information. Taufolio's cloud environments and cloud services must be protected from internal and external intrusion, at a level appropriate to the data they carry, to protect business data, application systems and platform software from unauthorized access. This procedure gives guidance for implementing the network security controls required by the Communications and Network Security Policy.

2. Scope

This procedure applies to all processes and operations at Taufolio within the scope of its information security management. Taufolio has no office network and no self-managed servers. Its perimeter consists of the edge network and firewall of its hosting provider (Vercel), the managed database platform (Supabase) and the connections between them, the subprocessors and brokerage providers.

3. Network security management

3.1 Network control

- The Information Security Officer is the designated owner of Taufolio's cloud environments and services, including hosting, database, authentication and the domain and DNS configuration.
- All public traffic enters through the hosting provider's edge network. Firewall rules and attack-mitigation settings in that platform must be configured to block abusive traffic, and their reports (traffic analysis, blocked requests, anomalies) must be reviewed regularly.
- All traffic to taufolio.com must use TLS 1.2 or higher, with HSTS enabled. Certificates are issued by a trusted public authority and must renew automatically.
- Calls from Taufolio's servers to the database, to subprocessors and to brokerage APIs must use TLS.
- The database is not publicly accessible. No anonymous access path exists: the legacy anonymous key and all publishable keys are disabled, no browser or mobile client talks to the database directly, and Row Level Security is enabled on every table in the public schema. Direct connections must be restricted to the application and to named administrators, and SSL must be enforced on them.
- Any change to network, firewall or domain configuration must follow the change management process in the Operations Security Procedure.
- Logs and alerts of the providers' security tooling (the Vercel firewall and Supabase security advisors) must be reviewed regularly. Any anomaly must be raised as an information security incident and handled through Taufolio's incident response process.
- The Information Security Officer must ensure that data passing through the network is encrypted wherever feasible.

3.2 Security of network services

- The Information Security Officer must define the security requirements for network services. They include at least encryption, attack mitigation and filtering at the edge, and monitoring.
- These requirements must be implemented for every cloud service used. When a network service is procured from a third-party provider, the requirements must be reflected in the provider's terms or in a data processing agreement, and the provider's own security attestations should be reviewed.
- A third-party independent assessment of the network perimeter (for example a penetration test) should be carried out annually to give assurance to management, users and partners and to meet regulatory expectations.
- Assessment results must be documented and any issue remediated. After allowing a reasonable time for remediation, a follow-up test must confirm that the issues were corrected.

3.3 Network access control

3.3.1 Use of network services

- Access to production environments and the administrative consoles of the hosting, database, authentication and source code providers must be restricted to named staff accounts that use multi-factor authentication.
- A list of the accounts that have access to production must be maintained in the access register kept by the Information Security Officer.
- The Information Security Officer must review access to production at least quarterly.

3.3.2 Remote administration

- Administrative access to infrastructure must go only through the providers' consoles and APIs, or through encrypted protocols such as TLS or SSH, using credentials tied to a named account. Shared accounts must not be used.
- Diagnostic and configuration services must not be exposed to the public internet.

3.3.3 Separation of environments

- Production must be separated from development and preview environments. Production data and production secrets must not be used in development or preview.
- Access to the production and development environments must be granted by role.
- Data flows between environments and services must pass through controlled, authenticated interfaces.

3.3.4 Remote devices

- Every device used to access production must meet the Endpoint Security Policy: current operating system and protection software, full-disk encryption, screen lock and a host firewall enabled.

- Staff members using public Wi-Fi must be aware that a device without a firewall can be attacked. Production must be accessed only over TLS connections, and a trusted VPN should be used on untrusted networks.

4. Document security classification

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

5. Non-compliance

Compliance with this procedure 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 procedure 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.

6. Responsibilities

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

7. Schedule

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

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

8. 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