



POLICY · INFRASTRUCTURE AND OPERATIONS

Operations 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. Operations security

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

The objective of this policy is to ensure the secure operation of Taufolio's production infrastructure and to prevent disruptions to the availability of Taufolio's services, through adequate planning, operating procedures, backups, change management, logging and vulnerability management.

2. Scope

This policy applies to all processes and operations at Taufolio within the scope of its information security management, in particular the production application hosted on Vercel, the production database and file storage on Supabase (EU, Ireland), and the supporting services that process Taufolio data (authentication, payments, email, monitoring and analytics).

3. Policy statement

Taufolio must take adequate precautions and design appropriate controls to prevent misuse of its information assets, and must ensure that operational activities do not affect the confidentiality, integrity or availability of its services. To this end Taufolio must maintain an appropriate level of information security, minimize the risk of system failures, protect the integrity of software and information, protect information in networks and infrastructure, prevent unauthorized disclosure, manage technical vulnerabilities, keep software and information that is exchanged secure, and detect unauthorized activity.

4. Operations security

4.1 Change management

- Formal change management must be in place for every change that can affect information security, including application code, production infrastructure, hosting and database configuration, and documented policies and procedures.
- The procedure must cover both scheduled and emergency changes.
- Changes must be recorded, reviewed and tested before they reach production. Records and approvals must be kept in a central system: the private GitHub repository (commits, pull requests, review history) for code and configuration, and the Taufolio issue tracker for other changes.
- Where the team has more than one member, the author of a change and its approver should be different people. While Taufolio is operated by a single person, compensating controls apply: automated tests, linting and type checks must pass before a change is released, and the change history must remain available for later review.
- Changes must be tested in an isolated environment (local development or a preview deployment) before they are released, to assess their impact on operations and security and to confirm that only intended changes were made.

- The production environment must be separated from other environments. Production secrets must not be available to development or preview environments.
- Modifications to vendor-supplied products should be avoided. Where a modification is unavoidable, it must be documented and the original must be retained.

4.2 Capacity management

- Critical parameters of the production service, such as response times, error rates, function execution limits and database load, must be monitored against defined thresholds at regular intervals to maintain performance and availability.
- Capacity planning must consider current usage and projected growth.
- System monitoring must be enabled, and detective controls such as alerts must be configured so that problems are signaled in good time.

4.3 Configuration management

- Configuration baselines for critical infrastructure and software must be established and documented where required. They cover hosting project settings, firewall rules, database settings and the hardening of staff endpoints.
- Any change to production configuration, firewall rules or database settings must follow the change management process in section 4.1.
- Time must be synchronized across cloud services and endpoints, using the providers' managed time sources, so that logs remain accurate and traceable.

4.4 Backups

- All original customer data must be backed up. Taufolio's database runs on Supabase, which creates automated backups; the backup frequency and retention must be set according to the risk to the service and Taufolio's commitments to customers.
- Backups must be stored outside the production database itself, in the provider's managed backup storage, and are protected with the same encryption at rest as the production data.
- A backup restoration exercise must be performed at least annually to confirm that backup data is readable and usable in an emergency.
- The documented backup procedure must define: the backup frequency and the frequency of restoration tests; the data to be backed up; the type of backup; the testing method; the instructions for restoring in a real disaster; and the retention period.
- Backups must be restored periodically and the results recorded. If a restoration test fails, the data owner must be notified and a root cause analysis carried out.
- Backups that contain customer credentials contain only application-encrypted values, because the encryption master key is not stored in the database. See the Encryption Policy.

4.5 Logging and monitoring

- Infrastructure and software must be configured, where feasible, to capture security-relevant events such as privileged account use, system failures, policy violations, unauthorized access attempts and firewall activity. Taufolio uses Sentry (EU region) for error and performance monitoring, together with the audit and request logs of its hosting, database and authentication providers.
- Customer credentials, access tokens, request bodies and portfolio contents must never be written to logs or sent to monitoring tools.
- Logging must take account of legal and contractual requirements. Evidence must be collected, retained and presented where legal action or a regulatory request follows an information security incident.
- Logs must be retained for the period required by applicable law and long enough to support incident investigation. Error monitoring data in Sentry is retained for 90 days.
- Logging facilities and log information must be protected against tampering and unauthorized access.

4.6 Control of operational software

Taufolio is deployed to managed platforms and does not operate its own servers. Software must reach production only through the controlled deployment pipeline described in section 4.1. Nothing may be installed on production infrastructure outside that pipeline.

4.7 Technical vulnerability management

- A documented procedure for technical vulnerability management must exist (see the Operations Security Procedure).
- Timely information about vulnerabilities in the infrastructure and software in use must be obtained from trusted sources, such as dependency advisories and provider security advisories.
- Where possible, tool-based vulnerability scans must be carried out for critical components.
- An independent assessment by a third party is recommended once a year.
- Timelines must be defined for responding to identified or reported vulnerabilities.
- Each vulnerability must be evaluated for risk, considering the criticality reported by the vendor or tool and the likelihood of exploitation (for example, a known public exploit), and then categorized as High, Medium or Low.
- If closing a vulnerability requires a patch, the patch must be tested before it is deployed to production, and the system must be checked to confirm that existing functionality is not affected.
- For High-risk vulnerabilities, a check must confirm that the vulnerability has been closed after the fix is applied.

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 Operations 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