



PROCEDURE · INFRASTRUCTURE AND OPERATIONS

Operations 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. Operations security procedure

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

The objective of this procedure is to ensure the operational security of Taufolio's services through defined steps for change management, backups, logging and monitoring, and vulnerability management. It implements the Operations Security Policy.

2. Scope

This procedure covers all systems in Taufolio's production environment: the application and its domains hosted on Vercel, the database and file storage on Supabase, and the supporting services (authentication, payments, email, monitoring and analytics) that process Taufolio data.

3. Operations security procedure

3.1 Change management

3.1.1 Version control

- All software developed for Taufolio, including infrastructure and configuration kept as code, must be held in version control (git) in Taufolio's private GitHub repository, so that the latest and every previous version is available.
- Work must be done on branches created from the current state of the central repository. All changes must be tested locally before they are released to users.

3.1.2 Initiating planned changes

- New features and fixes must be developed on a separate branch. A change is proposed for release through a commit history or pull request that shows the differences it introduces.
- Changes that are not code, such as a change to a hosting, database or firewall setting, must be tracked in the Taufolio issue tracker with the owner, the reason, the impact and the steps for rollback.

3.1.3 Approving planned changes

- Where a second reviewer is available, a change must be approved by someone other than its author. While Taufolio is operated by a single person, the author must review the full diff before release and the automated checks (tests, linting, type checks) must pass; their results are part of the change record.
- The review should ask at least the following, as far as they apply to the change:
 - Does the change solve the problem it set out to solve, and are all requirements met?
 - Could it have unintended consequences for other parts of the system?
 - Does it adversely affect the user experience?

- Does it contain algorithmic or logical errors?
- Does it require changes to the environment itself, such as new production environment variables?
- Could it cause performance problems?
- Could it be achieved in a more robust or less disruptive way?
- Secrets must never be committed to the repository. Production secrets must be set in the hosting provider's secret store and marked as sensitive.

3.1.4 Unplanned changes

- Unplanned changes, such as hotfixes, may be required when production is in an undesired state, for example a critical bug, an outage or a security issue.
- Depending on urgency, a hotfix may be released before a full review. It must then be reviewed after the fact.
- The commit or pull request message must describe the issue being fixed.
- Because every change is held in version control, an emergency change that causes unintended consequences can be rolled back by reverting it or redeploying the previous version.

3.2 Backup procedure

- Customer data in the production database must be backed up daily. Taufolio relies on the automated backups of its database provider, Supabase, and the Information Security Officer must confirm that backups are enabled.
- The backup retention period must be at least 7 days.
- A restoration test must be performed at least once a year to confirm that data is readable and complete. The test must be recorded, including which backup was restored and which sanity checks were run.
- Restoration tests are carried out by the administrators of the production infrastructure together with the Information Security Officer. A failed restoration test must be reported to the data owner and followed by a root cause analysis.
- A disaster recovery plan must exist so that systems can be recovered and returned to service after a major failure. It must be exercised at least once a year as a walkthrough led by the Information Security Officer.

3.3 Logging and monitoring procedure

- Application errors and performance problems are reported to Sentry (EU region). Request bodies and portfolio contents are not sent to it, and credentials must never appear in any log or report.
- The Information Security Officer must review provider audit logs (GitHub, Vercel, Supabase, Clerk) and monitoring alerts on a regular schedule and after any suspected incident.
- Alerts that indicate a possible security event must be handled as an incident through Taufolio's incident response process.

- Capacity indicators, such as error rates, response times and database load, must be checked regularly and when usage changes significantly.

3.4 Vulnerability management procedure

- Taufolio must monitor its dependencies continuously, through automated dependency updates and advisories on the source repository, and must review the security advisories published for its database platform (Supabase security advisors) on a regular schedule.
- The Information Security Officer must ensure that external vulnerability scans or penetration tests are performed periodically.
- All vulnerabilities found must be tracked together with their severity in the Taufolio issue tracker.
- Vulnerabilities must be remediated within the timelines the Information Security Officer defines for each severity. If a timeline is missed, the justification must be documented and the Information Security Officer must decide on further action.
- Vulnerabilities identified by external assessments must be tracked with the others until closed.
- Each vulnerability must be resolved with one of the following statuses:
 - **Fixed:** the vulnerability has been closed by a patch, an update or a system change.
 - **False positive:** the report has been investigated and found invalid.
 - **Vulnerable but unused:** the affected code or component is not in use, so the vulnerability is no longer a threat.
 - **Acceptable risk:** the vulnerability has been analyzed and does not pose a significant risk. This is a rare case, allowed only with extenuating circumstances or extremely high remediation cost, and the decision must be documented.

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 Operations 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