



POLICY · PRODUCT SECURITY

System Acquisition and Secure Development Lifecycle 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. System acquisition, development and maintenance

5. Security in development and support processes

6. System testing

7. Test data

8. Document security classification

9. Non-compliance

10. Responsibilities

11. Schedule

12. Version history

1. Objective

This policy provides a framework that keeps software development at Taufolio aligned with information security throughout the whole lifecycle. Taufolio is committed to building reliable systems and to treating security as an integral part of every phase of acquisition, development and maintenance, not as a step added at the end.

2. Scope

This policy covers the development process for the software that Taufolio builds or acquires, including the production application, its server-side code, database schema and integrations with third-party services (for example brokerage connectors). It must be followed by all staff members, contractors and partners who take part, wholly or partly, in product development.

3. Policy statement

Security must be considered at every stage of a system's life: feasibility, planning, development, implementation, maintenance, retirement and disposal. The aims are to:

- ensure conformance with all applicable security requirements;
- protect Taufolio and customer data throughout the development lifecycle;
- prevent the introduction of new risks when a system is modified;
- ensure that data is properly removed when a system or feature is retired.

4. System acquisition, development and maintenance

4.1 Software development life cycle

Security must be considered and included in every phase: requirements, design, development, testing, release, operations and maintenance. The detailed steps are set out in the Secure Development Procedure.

At Taufolio the following controls are in place today:

- Source code is kept in a private GitHub repository, and every change goes through version control.
- An automated gate runs on every change before it is pushed: formatting, lint, type checking and the unit tests related to the change.
- Every production release additionally runs the full unit test suite, the repository's security guard tests and the end-to-end test suite.
- Changes are reviewed before release, either by a person or by an independent automated code reviewer.

- Database schema changes are versioned migration files, applied deliberately and never automatically.
- Production deployments are explicit releases on Vercel, with instant rollback to the previous deployment.
- Secrets are never stored in the repository; a pre-commit secrets scan blocks them.

4.2 Requirements

- Security and privacy requirements for a new feature or system must be defined when its requirements are defined.
- Legal and regulatory implications, and security requirements for any confidential or personal data the feature collects or uses, must be considered. Features that touch customer credentials or brokerage data must follow the Encryption Policy.
- Requirements for reliability and availability must be considered. Where the existing architecture cannot deliver the required availability, redundant components or alternative architectures should be evaluated.

4.3 Design

- Threats and potential vulnerabilities must be identified early in design, including ways the feature could be misused and ways protective measures could be bypassed.
- The operating environment, the internal and external interfaces, the components and the data flowing between them must be identified.
- Software must be designed to run with the minimum privileges necessary. Application permissions and access controls must follow the defined user roles.
- Third-party services that would receive personal data must be assessed under the Vendor Management Policy before they are integrated.

4.4 Development

- Development must take place in an environment that is separate from production, with its own credentials. Production credentials must never be used in development.
- Developers must take care to validate incoming and outgoing data, apply secure authentication and session handling, and use sound error and exception handling.
- Source code must be protected from unauthorized access. The repository must remain private, accounts with access must use multi-factor authentication, and version control must record every change.

5. Security in development and support processes

5.1 Secure application development principles

Taufolio applies the following secure development principles:

- use current best practices and maintained libraries for each language and framework in use;
- protect the version control system and the code repository;
- keep staff members who write code trained in secure coding;
- enable developers to avoid, find and fix vulnerabilities wherever possible.

5.2 Change control

- Changes to systems must be controlled through formal change control. New systems and major changes must follow documentation, specification, testing, managed implementation and quality control.
- Each change must be assessed for its impact and for the security controls it needs, and it must not weaken existing security procedures.
- Access of developers and support staff must be limited to the parts of the system their work requires.
- Before a change is released the following must be confirmed:
 - it was submitted by an authorized person and approved before implementation;
 - existing controls and integrity procedures are not compromised;
 - all software, data entities and infrastructure that need amendment are identified;
 - critical code is checked to limit known security weaknesses;
 - system documentation is updated where applicable;
 - a record of the change exists in version control.
- Dependency and platform updates must be applied through the same change process. Updates to critical systems must not be applied blindly: the risk to integrity and availability must be weighed against the benefit of rapid deployment.
- After a change to an underlying platform, business-critical functions must be reviewed and tested for adverse effects on operations or security.
- Vendor-supplied software and libraries should be used without modification wherever possible. Where modification is unavoidable, the risk to built-in controls, the burden of future maintenance and compatibility with other software must be considered, and the original must be retained.

5.3 Secure engineering

- Security principles must be applied at every architecture layer (business, data, application and technology), balancing security with accessibility.
- New technology must be analyzed for security risks, and designs reviewed against known attack patterns.
- Systems must be reviewed regularly so that they stay current against new threats.
- Where development is outsourced or relies on a third party, security requirements must be passed on through contracts and agreements.

5.4 Secure development environments

The Information Security Officer must establish and protect secure environments for development and integration across the whole lifecycle. A secure environment covers people, processes and technology. For each development effort the following must be considered:

- the sensitivity of the data processed, stored and transmitted;
- applicable legal, regulatory and internal requirements;
- security controls already in place;
- the trustworthiness of the people working in the environment;
- the degree of outsourcing involved;
- the need to separate environments from one another;
- control of access to each environment;
- storage of backups in secure locations (production backups are provided by the database provider);
- control over the movement of data into and out of the environment.

6. System testing

- New and updated systems must be tested and verified during development, with defined inputs and expected outputs across a range of conditions.
- The author of a change tests first. Independent verification must then take place before the change reaches production: the automated test suites, and review by a person or by an independent automated code reviewer.
- The extent of testing is decided by the Information Security Officer in line with the importance and nature of the system. Integrated behavior, and not only individual units, must be tested.
- Automated tools such as static analysis, type checking, dependency scanning and the repository's security guard tests should be used, and the remediation of defects must be verified.
- Testing must be carried out in an environment that cannot introduce vulnerabilities into production.
- Before the first external audit of the controls in this policy, an independent penetration test must be performed. Findings must be tracked to closure.

7. Test data

- Customer data is never used in development or testing. Tests must use synthetic or fixture data.
- Where a test needs data shaped like operational data, personal and confidential content must be removed or replaced before use.
- Access controls that apply to production systems apply equally to any test system that holds sensitive data.

- Any operational data that is unintentionally copied to a test environment must be erased immediately after use, and the incident must be reported to the Information Security Officer.

8. Document security classification

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

9. Non-compliance

Compliance with this policy is verified through the automated change gate, code review, 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.

10. 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.

11. Schedule

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

End of System Acquisition and Secure Development Lifecycle Policy. For the version history, see the next page.

12. 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