



POLICY · RESILIENCE AND INCIDENT RESPONSE

Incident Management 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. Information security incident management

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

The objective of this policy is to provide a framework within which information security events and incidents affecting Taufolio's systems are communicated in a timely manner and the necessary corrective actions are taken. Taufolio handles sensitive material, in particular the credentials users grant it to read their brokerage accounts, so a fast and orderly response is a core part of protecting users.

2. Scope

This policy applies to all processes, systems and operations of Taufolio within the scope of its Information Security Management System, to all staff members (employees and contractors), and to the subprocessors that process Taufolio data on its behalf.

3. Policy statement

Security incidents are irregular and anomalous conditions that cause, or may lead to, service degradation, loss or exposure of sensitive data, outages or any other form of reduced operational status. Such situations require prompt human intervention to avert disruption or to restore normal operation.

This policy establishes the principles for handling incidents. It guides staff members and incident responders who believe they have discovered, or are responding to, a security incident. The detailed steps are set out in the Incident Management Procedure.

4. Information security incident management

4.1 Responsibilities and procedures

- An Incident Management Procedure must be maintained to define the procedures and responsibilities that ensure quick, effective, consistent and orderly responses to information security incidents.
- The Information Security Officer is responsible for:
 - investigating and coordinating reported information security incidents and security weaknesses;
 - tracking the closure of incidents and of the corrective and preventive actions that result from them.

4.2 Reporting information security events and incidents

- Taufolio must provide channels through which information security events and incidents can be reported as quickly as possible. These include email to support@taufolio.com, the in-app "Report a problem" form for users, and direct contact with the Information Security Officer for staff members.
- Every information security incident must be recorded in the incident register kept by the Information Security Officer.

- The steps for reporting an incident must be communicated to all staff members and must be easy to find and use, for reporting both incidents and security weaknesses.
- Monitoring must be in place for the proactive detection of intrusions, attacks and fraud, using error monitoring, firewall and runtime logs, database logs and security advisories, and product analytics, as described in the Incident Management Procedure.

4.3 Assessment of and response to incidents

- Every reported incident must be assessed and classified against the criteria in the Incident Management Procedure.
- The assessment and classification must be retained so that similar events can be identified quickly and false positives avoided.
- A response plan must cover the full incident cycle: identification, containment, root cause analysis, resolution and recovery.
- The response must identify corrective action wherever it matters.
- Where a follow-up action against a person or organization involves legal action, civil or criminal, evidence must be collected, retained and presented in line with the rules of evidence of the relevant jurisdiction.
- Where an incident involves personal data, the Data Breach Notification Policy applies in addition to this policy.

4.4 Learning from incidents

- Incidents must be analyzed, and the analysis shared with management and, where appropriate, with the relevant authorities and affected partners.
- Knowledge gained from resolving incidents must be used to reduce the likelihood and the impact of similar incidents in the future.

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, 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 and for reporting incidents and weaknesses without delay.

8. Schedule

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

End of Incident Management 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