



PROCEDURE · RESILIENCE AND INCIDENT RESPONSE

Incident Management 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. Information security incident management

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

The objective of this procedure is to establish a consistent and effective approach to managing incidents throughout their lifecycle: identification, assessment, containment, corrective action and closure.

2. Scope

This procedure applies to all staff members performing operations within the scope of Taufolio's Information Security Management System, and to all production systems: the application hosted on Vercel, the Supabase database and file storage, Clerk authentication, and the connections to brokerage providers (SnapTrade and the direct tastytrade and Interactive Brokers connectors).

3. Information security incident management

3.1 Responsibilities

- The Information Security Officer investigates and coordinates reported incidents and security weaknesses, and tracks closure of incidents and of the corrective and preventive actions that follow.
- The Information Security Officer is accountable for ensuring that every incident is dealt with appropriately.
- Where Taufolio engages additional engineers or contractors, the Information Security Officer assigns them to an incident as needed. Staff members assigned to an incident must follow the Information Security Officer's instructions.

3.2 Detection and reporting

Where feasible, monitoring must be in place for the proactive detection of intrusions, attacks and fraud. Incidents are detected or reported through the following sources:

Source	What it provides
Sentry alerts	Application errors and performance anomalies (request bodies and portfolio contents are not sent to Sentry)
Vercel firewall and runtime logs	Suspicious traffic, blocked requests, runtime errors and failed deployments
Supabase logs and security advisors	Database and authentication anomalies, and advisories on access-control weaknesses
PostHog	Unusual usage patterns in product analytics
User reports	The in-app "Report a problem" form and email to support@taufolio.com

Source	What it provides
Staff reports	Any weakness or event observed by a staff member, reported directly to the Information Security Officer
Provider notices	Security notifications from subprocessors and brokerage partners

Rules for reporting:

- Staff members must report any observed incident or weakness immediately, by email or directly, and must not wait to be certain.
- If a staff member notices malicious behavior by another staff member or by a partner, they must report it directly to the Information Security Officer and should not discuss it with anyone else.
- User reports arriving through the in-app form are triaged with the help of an AI assistant. A report that mentions a possible security problem must be escalated to the Information Security Officer immediately.
- A log of all reported security incidents must always be maintained in the incident register.

3.3 Severity classification

The Information Security Officer, as the first point of contact, assesses the severity of every incident:

- **Low.** Does not require immediate remediation. Typically a partial loss of a Taufolio feature for which a workaround exists. Handled in normal working time.
- **Medium.** Similar to Low, but may include suspicious emails, unusual activity on a staff device, or an anomaly with no sign of data exposure. Does not require immediate remediation. Low and medium incidents are expected to be the large majority.
- **High.** An active attack has not yet succeeded but is likely, or a significant weakness is being exploited. Examples: a backdoor, malware, a leaked secret, malicious access to business data such as passwords, payment information or vulnerability data. Immediate remediation must begin.
- **Critical.** An attack was successful and something important was lost, or irreparable damage was done to production services. Examples: confirmed exposure of customer data or of brokerage credentials. Immediate action must be taken to limit the damage.

For High and Critical incidents, the Information Security Officer must immediately involve every stakeholder who is needed, including affected subprocessors and partners.

3.4 Response and resolution

1. **Record.** Open an entry in the incident register with the time of detection, the source, a description and the initial severity.
2. **Contain.** Stop the harm first: revoke or rotate affected credentials, block abusive traffic at the Vercel firewall, disable an affected feature or integration, or roll back to a previous deployment.

3. **Investigate.** Establish what happened, which systems and data are affected, and since when, using provider audit logs and the logs listed in section 3.2.
4. **Eradicate and recover.** Remove the cause, restore normal service (see the Business Continuity Plan), and confirm through monitoring that the problem does not recur.
5. **Notify.** If personal data is involved, follow the Data Breach Notification Policy and the Personal Data Breach Notification Procedure. If a brokerage partner is affected, notify it as the contract requires.
6. **Close.** Record the investigation, the corrective actions and the closure date.

For incidents with no data loss and no direct impact on availability, the details of the investigation and the corrective actions are documented in the closure notes.

For Critical incidents the response follows an iterative process of investigating, containing the exploitation, remediating the vulnerability, and writing a post-incident review. In addition:

- The Information Security Officer decides whether legal counsel must be involved under privilege.
- A timeline of known facts must be created, stating what is known about the attacker's actions and when they occurred.
- Long-term mitigations must be recommended to avoid a similar incident.
- Where customer data was lost or stolen, Taufolio must communicate with the affected users.

3.5 Playbook: suspected credential compromise

This playbook applies when a user's brokerage credentials, or the key that protects them, may have been exposed. Customer credentials are encrypted at the application layer, and the master key is held only in the hosting provider's secret store, so a leaked copy of the database alone does not expose them. A suspected compromise of the master key, of the hosting secret store, or of the server runtime must nevertheless be treated as Critical until ruled out.

1. **Declare and record.** Open a Critical entry in the incident register.
2. **Revoke at the broker.** Revoke the affected OAuth tokens, API keys and user secrets at the brokerage provider (SnapTrade, tastytrade or Interactive Brokers) for every affected user, using the provider's revocation mechanism. Where the scope is unclear, revoke for all users of that provider.
3. **Disable the connector.** Temporarily disable synchronization for the affected provider so that no further calls are made with possibly exposed credentials.
4. **Rotate the master key.** Generate a new master key and place it in the hosting provider's secret store marked as Sensitive. The previous key stays available for decryption only for the duration of the next step.
5. **Re-encrypt.** Re-encrypt every stored secret under the new master key, verify that all records decrypt, and then destroy the previous key. If the compromise affected the stored ciphertexts rather than the key, delete the affected credentials and require users to reconnect.
6. **Rotate related secrets.** Rotate the database secret key, the authentication provider secrets and any other secret that shared an exposure path with the compromised one.

7. **Investigate.** Review Vercel, Supabase, Clerk and GitHub audit logs to establish the cause, the time window and whether any credential was used by an unauthorized party. Check broker-side activity where the provider makes it available.
8. **Notify.** Notify affected users without undue delay, with instructions to review their brokerage accounts and, if necessary, change their broker passwords. Notify the brokerage partner according to the contract. If personal data was affected, follow the Personal Data Breach Notification Procedure, including the 72-hour supervisory authority deadline.
9. **Recover and review.** Restore the connector, ask users to reconnect where credentials were deleted, and complete the post-incident review described in section 3.6.

3.6 Learning from critical incidents

- For Critical incidents the Information Security Officer must analyze the cause, effect, mitigation and lessons learned, and share the analysis with management and, where appropriate, with the relevant authorities and partners.
- Knowledge gained must be documented and used to reduce the likelihood and impact of similar incidents.
- Where possible, the analysis should consider the costs caused by the incident.
- The output must be used to improve the security posture and to understand recurrence and impact tolerance.

3.7 Collection of evidence

- Where a follow-up action involves legal action, civil or criminal, evidence must be collected, retained and presented according to the rules of the relevant jurisdiction.
- Until the seriousness of an incident is understood, care must be taken that evidence is not destroyed, intentionally or accidentally. Relevant logs must be exported before any retention period ends.

3.8 Contact with authorities and special interest groups

- The Information Security Officer must maintain contact with the relevant authorities, including the Polish President of the Personal Data Protection Office (UODO), law enforcement and cyber security response teams, and with affected partners.
- As the applicable regulations require, the Information Security Officer must report observed incidents to the appropriate authorities promptly.
- Taufolio should follow security advisories of its providers and of security communities to improve knowledge of best practices, receive early warnings of attacks and vulnerabilities, and exchange information about new threats.

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, 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 policies. Staff members are responsible for applying the relevant sections of this procedure 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 Incident Management 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