



POLICY · RESILIENCE AND INCIDENT RESPONSE

Business Continuity and Disaster Recovery 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 aspects of business continuity management

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

The objective of this policy is to set out guidelines for Taufolio's business continuity and disaster recovery. It prescribes the requirements for planning recovery from disasters so that Taufolio's commitments to its users and partners can be met.

2. Scope

This policy applies to all processes and operations of Taufolio within the scope of its Information Security Management System, including the production application on Vercel, the Supabase database and file storage, authentication, payments, email and the connections to brokerage providers.

3. Policy statement

Taufolio aims to provide a dependable service to its users. Continuity of operations, in a secure manner, must therefore be planned for and embedded in Taufolio's business continuity management and disaster recovery planning. Taufolio relies on managed cloud providers for much of its resilience, and this policy requires that reliance to be understood, documented and tested.

4. Information security aspects of business continuity management

4.1 Information security continuity

4.1.1 Planning information security continuity

- Information security processes must include requirements that preserve the confidentiality, integrity and availability of critical information assets even during a business disruption or disaster.
- Taufolio must define recovery guidelines, including recovery time and recovery point targets, that serve as a baseline for classifying mission-critical systems and for developing recovery and restoration plans.
- A strategy for the overall business continuity and disaster recovery approach must be maintained. Information security controls that apply in normal operation must stay in force during a disaster. Any exception requires the approval of the Information Security Officer.
- Taufolio must maintain readiness of its information and communication technology through regular backups, the redundancy and failover capabilities of its managed providers, automated monitoring, incident response procedures and recovery strategies that keep downtime to a minimum.
- Infrastructure and database schema must be defined in the version-controlled repository, so that the service can be rebuilt reproducibly.
- These measures must be tested through exercises, reviewed for continuous improvement, and updated to maintain the resilience and availability of essential services.

4.1.2 Implementing information security continuity

- Taufolio must ensure that an adequate framework is in place to prepare for, mitigate and respond to a disruptive event, using people who have the necessary authority, experience and competence.
- Personnel with responsibility, authority and competence to manage an incident and maintain information security must be identified, and a deputy must be named for each of them wherever the organization size allows.
- Comprehensive, well-documented plans, response strategies and recovery procedures must be developed and approved to manage and limit the impact of any disruptive event. The Business Continuity Plan fulfils this requirement.

4.1.3 Verify, review and evaluate information security continuity

- Information security controls of all systems and sites that take part in continuity must be reviewed and verified.
- Business continuity plans must be tested and updated regularly to make sure they remain current and effective.
- The roles and responsibilities for contingency planning and recovery must be reviewed and updated at least annually.

4.2 Redundancy

- Taufolio must identify its business requirements for the availability of information systems.
- Redundant components or architectures must be considered wherever availability cannot be assured by the existing architecture, including reliance on the redundancy offered by the hosting, database and content delivery providers.
- Failover and restore mechanisms must be tested to confirm that they work.

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 recovery exercises, 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 Business Continuity and Disaster Recovery 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