



PROCEDURE · RESILIENCE AND INCIDENT RESPONSE

Business Continuity Plan

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. Plan objectives

4. Assumptions

5. Disaster definition

6. Preparation for disaster recovery and business continuity

7. Instructions for using the plan

8. Document security classification

9. Non-compliance

10. Responsibilities

11. Schedule

12. Version history

1. Objective

The objective of this plan is to prepare Taufolio for extended service outages caused by factors beyond its control, such as failures at a hosting or database provider, natural events or man-made events, and to restore services to the widest extent possible within an acceptable time frame.

2. Scope

The scope of this plan is limited to business continuity and disaster recovery of Taufolio's production infrastructure: the application hosted on Vercel, the Supabase database and file storage (EU, Ireland), and the services on which they depend, such as Clerk, Stripe and Resend.

3. Plan objectives

- Serve as a guide for whoever carries out recovery.
- Reference and point to the location of critical data and configuration.
- Describe the procedures and resources needed for recovery.
- Identify the vendors, partners and users that must be notified in the event of a disaster.
- Avoid confusion in a crisis by documenting, testing and reviewing recovery procedures in advance.

4. Assumptions

- The Information Security Officer, or a named deputy, is available following a disaster.
- A national-scale catastrophe is outside the scope of this plan.
- This document and the other vital records are stored where they survive an outage of Taufolio's own systems and are accessible immediately afterwards, for example in the source code repository and in a copy held outside the production environment.
- Each provider on which Taufolio depends maintains its own continuity and recovery plans.

5. Disaster definition

A disaster is any loss of utility service, connectivity or hosting capability, or any catastrophic event, including a provider outage, a destructive attack, data corruption or accidental deletion, that causes an interruption in the service provided by Taufolio and that is not likely to be resolved within the time frames in section 6.2. The plan identifies vulnerabilities and recommends measures that prevent extended outages.

6. Preparation for disaster recovery and business continuity

6.1 Recovery mechanisms

Concern	Mechanism
Application	Every deployment on Vercel is kept, so service can be restored by an instant rollback to a previous known-good deployment
Application and infrastructure definition	Source code, configuration and database schema are defined in the version-controlled, private repository on GitHub, so the service can be rebuilt reproducibly
Database and file storage	Supabase manages automated backups, and the database can be restored from them
Secrets	Held in the hosting provider's encrypted secret store; the master key for customer credentials is held separately from the database, and a copy of it must be kept in a secure location outside the production environment so that stored credentials remain recoverable
Brokerage connections	If credentials cannot be recovered, they are deleted and users reconnect their accounts

6.2 Recovery targets

These are targets that guide planning and exercises. They are not contractual guarantees.

- **Recovery time objective (RTO):** 24 hours for the core service.
- **Recovery point objective (RPO):** 24 hours, the maximum period of data changes that may be lost.

The targets must be evaluated and adjusted through recovery exercises, and the results recorded.

6.3 Preparation

- Backups must be taken frequently and stored at a location redundant to the production database. The Information Security Officer must verify that automated backups are enabled and are succeeding.
- A backup restoration exercise must be performed at least annually, restoring a backup to a separate project to confirm it can be restored and to measure how long it takes.
- A disaster recovery drill, which may be a tabletop exercise, must be conducted at least annually so that the plan can be invoked effectively. The drill must evaluate the RTO and the RPO.
- The rollback of a deployment must be practiced so that it can be executed under pressure.

7. Instructions for using the plan

7.1 Invoking the plan

This plan becomes effective when a disaster is declared.

7.2 Disaster declaration

The Information Security Officer is responsible for declaring a disaster and for starting the recovery steps. A disaster must be declared only if the situation is not likely to be resolved within the time frames in section 6.2. Where a deputy has been named, the deputy may declare a disaster if the Information Security Officer is unavailable.

7.3 Recovery steps

Once a disaster is declared, recovery follows the Incident Management Procedure and the change management practices, in this order of preference:

1. Roll back to the previous known-good Vercel deployment if the cause is a faulty release.
2. Rebuild or redeploy from the version-controlled repository if the hosting configuration was lost.
3. Restore the database or file storage from the provider's managed backups if data was lost or corrupted, then verify integrity.
4. Rotate and re-provision secrets if their exposure is suspected, as described in the credential compromise playbook of the Incident Management Procedure.
5. Verify that the service works end to end, including authentication, payments and brokerage connections, before declaring recovery complete.

7.4 Notification of an incident or disaster

- Any staff member who notices a technical or operational incident must report it as soon as possible to the Information Security Officer by email or directly. The incident is then reviewed and resolved in accordance with the Incident Management Policy.
- The Information Security Officer must be notified promptly when any of the following occurs:
 - any security incident;
 - any production service is down for three or more hours;
 - any problem that would cause one of the above, or any clear indication that one is about to occur.
- The Information Security Officer is responsible for communicating the disaster and the successful recovery to the stakeholders concerned, which may include users, brokerage partners, subprocessors and regulators, as applicable. Where personal data is affected, the Data Breach Notification Policy applies.

7.5 Plan review and maintenance

This plan and the disaster recovery drill must be reviewed at least once a year, and after every disaster declaration or significant change in the infrastructure.

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 plan 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 plan 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 plan and the related policies, for organizing the recovery exercises, and for declaring a disaster. Staff members are responsible for applying the relevant sections of this plan 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 Business Continuity Plan. For the version history, see the next page.

12. 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