



PROCEDURE · THIRD PARTIES AND COMPLIANCE

Vendor 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. Vendor management procedure

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

This procedure sets out the responsibilities and the process for managing relationships with third parties and vendors that are critical to Taufolio's services.

2. Scope

This procedure applies to all staff members who use vendors whose services are critical to the operational integrity and availability of Taufolio's services, or with whom critical data is shared.

3. Vendor management procedure

3.1 Responsibilities

The Information Security Officer must ensure that:

- all Taufolio vendors and suppliers are identified;
- the security controls of a third party are vetted before a relationship is established;
- an agreement is in place with every vendor that processes personal data, and that it is current;
- a current and accurate list of vendors is maintained;
- vendors are monitored for adherence to their agreements, service levels and security requirements;
- the security measures of critical vendors are reviewed periodically or continuously.

Any staff member who wants to start using a new vendor, or learns of a change in an existing vendor's service, must notify the Information Security Officer before the change takes effect.

3.2 Contracts and service levels

- Once a vendor is selected, a contract must be signed with it where one is available. Most software-as-a-service vendors offer standard terms accepted online instead of a negotiated contract. In that case the Information Security Officer must review the vendor's published terms of service, security documentation and data processing terms.
- Vendors that process personal data on Taufolio's behalf must be bound by a data processing agreement. Where the vendor is outside the EEA, the transfer mechanism (adequacy decision or standard contractual clauses) must be identified and recorded.
- The Information Security Officer must ensure that confidentiality terms are in place with vendors that have access to sensitive data. Where that is not possible, the vendor's published privacy policy must be reviewed.

3.3 Vendor risk management

The list of vendors is maintained by the Information Security Officer and reviewed at least once a year. Each vendor is evaluated on:

- the impact on Taufolio's operations if the vendor's service is unavailable or breached;
- the vendor's access to customer data and other sensitive information.

Vendors are also assessed for suitability against these questions:

- Is there a way to contact the vendor during an interruption or degradation of service?
- Does the vendor hold information security certifications or attestations, such as SOC 2 or ISO/IEC 27001?
- Is enough information available about the vendor's security practices?
- If not, does the vendor need to complete a security questionnaire?
- What are Taufolio's options if the vendor has downtime or ceases to operate? Are there alternative vendors?

Based on the evaluation, each vendor is rated for criticality:

Rating	Meaning
High	Critical services are disrupted if the vendor fails, or the vendor has access to most or all critical data
Medium	Critical services keep working, and the vendor has restricted access to critical data
Low	Minimal impact on critical services, and minimal access to data

Depending on business need and the risk of the data involved, the vendor's certificates or security reports must be collected, and the Information Security Officer must check that they are valid. For every high-rated vendor, due diligence is mandatory: a review of the vendor's security certifications or attestations, or a security questionnaire.

3.4 Monitoring and review

- The Information Security Officer must review the vendor list and each vendor's rating at least annually.
- Anyone who monitors a vendor's service and notes a deficiency must inform the Information Security Officer immediately so that corrective measures can be taken.
- Changes to a vendor's sub-processors, locations, terms or security posture must trigger a re-assessment.

3.5 Current subprocessors

The following vendors process personal data on Taufolio's behalf. The list is reflected in the Taufolio privacy policy, which is the authoritative source for what data each vendor receives. It is updated when a vendor is added, removed or changed.

Subprocessor	Purpose	Data location
Vercel	Hosting, serverless compute, CDN and edge firewall	Global edge network
Supabase (PostgreSQL)	Primary database and file storage	EU (Ireland, eu-west-1)
Clerk	User authentication and session management	Provider-managed; processing outside the EEA is covered by standard contractual clauses
Stripe	Payments and subscriptions; Taufolio does not store card data	Provider-managed; processing outside the EEA is covered by standard contractual clauses
Resend	Transactional and broadcast email	Provider-managed; processing outside the EEA is covered by standard contractual clauses
PostHog	Product analytics and session replay, only after cookie consent	EU region
Sentry	Error and performance monitoring; no request bodies or portfolio contents; 90-day retention	EU region (Frankfurt, Germany)
GitHub	Source code, version control and code review (no customer data)	Provider-managed
Amazon Web Services (AWS Bedrock)	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
Anthropic	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
Google Cloud Vertex AI	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
Microsoft Azure AI Foundry	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
Microsoft Azure OpenAI	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
Microsoft Azure Document Intelligence	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA

Subprocessor	Purpose	Data location
OpenAI	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
OpenRouter	AI models for reports, summaries and document processing	Not pinned to the EEA; treated as outside the EEA
SnapTrade (Passiv Inc.)	Read-only brokerage connection aggregator	Canada (European Commission adequacy decision); may also process in the United States

Data sent to AI model providers is described, feature by feature, in the privacy policy, and anything sent to them must be treated as leaving the EEA. Credentials, passwords and payment-card data are never sent to any of them.

3.6 Brokerage partners

tastytrade and Interactive Brokers are brokerage partners whose accounts users choose to connect to Taufolio with read-only access. They are not subprocessors: they are data sources that the user authorizes, and Taufolio receives data from them only on the user's instruction. Taufolio requests read-only scopes (positions, balances and transactions) and never requests trading, order-placement, withdrawal or transfer permissions. Credentials issued by these partners are encrypted as described in the Encryption Policy and are deleted when the user disconnects the account or deletes their Taufolio account.

These partners are assessed under this procedure as vendors on which Taufolio's brokerage features depend, and their API or OAuth terms must be reviewed by the Information Security Officer before a connection goes live.

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 reviews of the vendor register, provider audit logs, periodic internal reviews and feedback to the policy owner. Any staff member found to have violated it 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 policy. 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 Vendor 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