



POLICY · THIRD PARTIES AND COMPLIANCE

Vendor 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. Vendor management

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

Taufolio depends on third-party vendors for a range of services, including hosting, database, authentication, payments, email, analytics, AI models and brokerage connectivity. Some of these services are critical to Taufolio's ability to meet its security commitments and to provide an uninterrupted service to its users. This policy sets the rules for managing vendor relationships so that the risk of using third parties is kept low.

2. Scope

This policy applies to vendors whose services are critical to the operational integrity and availability of Taufolio's services, and to vendors with whom customer or other critical data is shared. It also covers the third-party brokerage services that users authorize Taufolio to read from.

3. Policy statement

Taufolio exercises caution when it shares data with third parties. Every instance of data shared with a vendor widens the attack surface of that data. Taufolio relies on several third-party services and must therefore share some data, and it does so through a deliberate process: critical vendors are evaluated before use, bound by agreements, and reviewed regularly. Only the data a vendor needs for its purpose may be shared with it.

4. Vendor management

4.1 Information security in vendor relationships

- Information security requirements that reduce the risk of a vendor's access to Taufolio's assets must be agreed with the vendor and documented in an agreement, a data processing agreement or the vendor's published terms.
- Resilience and, where necessary, recovery and contingency arrangements must be defined for the information or processing the vendor provides.
- Vendor personnel with access to Taufolio assets must be bound by confidentiality, and must follow Taufolio's information security requirements where they work with Taufolio systems.
- The security controls and service levels in the agreement must be implemented, operated and maintained by the vendor.
- Where a vendor processes personal data on Taufolio's behalf, a data processing agreement under the GDPR must be in place, and transfers outside the European Economic Area must rely on an appropriate mechanism, such as an adequacy decision or standard contractual clauses.
- Confidentiality or non-disclosure terms that protect Taufolio's information assets must apply to vendors, to their subcontractors and to other third parties as applicable.

- Data shared with AI model providers must be limited to what is described in Taufolio's privacy policy. Customer credentials, passwords and payment-card data must never be sent to an AI model provider.

4.2 Vendor risk assessments and service delivery reviews

- A list of all vendors that are critical to Taufolio's services, or with which critical data is shared, must be maintained.
- Each vendor on the list must be assessed for its criticality to the service and for the sensitivity of the data shared with it.
- Where required, Taufolio may review a vendor's services through review calls, security documentation or audits. This is expected to be needed only in exceptional cases.

4.3 Reviewing vendors and managing changes to vendor services

- The vendor list and the risk assessments must be reviewed at least annually.
- Anyone who plans to adopt a new vendor, or learns of a change in a vendor's service level or terms, must tell the Information Security Officer before the change takes effect.
- Each such change must be followed by an update of the vendor list and a re-assessment of the risk.

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 reviews of the vendor register, 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 Vendor 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