



POLICY · PEOPLE

HR Security 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. Human resource security guidelines

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

The objective of this policy is to ensure that staff members and external parties understand their responsibilities for the roles they are considered for, are aware of their information security responsibilities and fulfill them, and that Taufolio's interests are protected when employment or engagement changes or ends.

2. Scope

This policy applies to all staff members, meaning employees (full-time and part-time) and external parties such as contractors and other third parties, who have access to Taufolio information systems.

3. Policy statement

Taufolio must ensure that staff members understand the responsibilities of their roles and are aware of and fulfill their information security responsibilities. Taufolio must also protect its interests, and the data of its users, when engagement changes or ends.

4. Human resource security guidelines

4.1 Before engagement

- As part of the hiring process, the competence of every candidate must be evaluated to ensure they can perform the expected responsibilities.
- Before starting work, every employee and contractor must sign the terms of engagement, which include their information security responsibilities and related obligations, during and after the engagement.
- Background verification checks should be performed on prospective staff members where permitted by law.
 - The extent of the checks must be proportionate to business requirements, the classification of the information to be accessed and the perceived risk. They may include checks of previous employment, confirmation of claimed qualifications, identity checks or, where lawful, criminal record checks.
 - Where background checks are not permitted or are disproportionate, a reference check may be used instead, depending on the level of information the person can access.
 - Staff members with access to production systems or customer data must be subject to at least an identity check and a reference check.
- Contractors and external parties must be assessed for their information security practices as part of vendor risk assessment, taking into account privacy, personal data protection and applicable

employment law. See the Vendor Management Policy.

4.2 During engagement

- Information security roles and responsibilities must be defined and documented for all staff members.
- All staff members must receive appropriate awareness training on organizational policies and procedures, including security requirements, legal responsibilities and acceptable use of Taufolio systems.
- Awareness training and formal information security training must be provided on joining and at least once a year thereafter. Training must cover the handling of customer credentials and personal data, phishing, and incident reporting.
- Taufolio's policies and training material must be available to all staff members.
- The Information Security Officer is responsible for implementing the information security controls and for monitoring that staff members comply with them.
- Staff members must report suspected security events and incidents promptly to the Information Security Officer.

4.3 Termination or change of engagement

- On departure, staff members must return or hand over all Taufolio assets under their control and either return or securely delete Taufolio data held on personal devices.
- On departure, all access rights and privileges to critical systems granted to employees or contractors must be revoked immediately, in line with the Access Control Policy.
- On a change of role or status, access rights and privileges must be reviewed and adjusted accordingly.
- Confidentiality obligations continue after the engagement ends.

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, records of training and acknowledgment, 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 the 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 HR Security 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