



PROCEDURE · PEOPLE

HR Security 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. HR security procedure

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

This procedure describes how information security is handled for staff members across their time with Taufolio: before engagement, during engagement and at its end. It implements the HR Security Policy.

2. Scope

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

3. HR security procedure

3.1 Before engagement

1. Before an offer or contract is issued, the Information Security Officer evaluates whether the candidate can perform the role. The evaluation is documented as a hiring evaluation and kept after the person joins.
2. The Information Security Officer ensures that the signed terms of engagement, including information security obligations, are in place before any access is granted.
3. Background verification, as defined in the HR Security Policy, is started at the time of joining. The results are documented and retained, within the limits of applicable law.

3.2 During engagement

1. After joining, the Information Security Officer onboards the staff member onto the necessary tools and systems and grants access according to the Access Control Procedure, with MFA enabled.
2. A role and a point of contact are assigned, and the list of active roles and their descriptions is documented and maintained.
3. New staff members must read and acknowledge the organizational policies, and complete the information security awareness training, within 30 days of joining. Completion is tracked in the internal records kept by the Information Security Officer.
4. At least once a year, the Information Security Officer requests that all staff members repeat the training and re-acknowledge the policies, and tracks completion.
5. Each staff member's performance of their job and information security responsibilities is evaluated at least once a year. The evaluation is documented and retained.

3.3 Termination or change of engagement

When a staff member decides to leave, or when the engagement is ended, the last working day is agreed with the Information Security Officer. On that day, at the latest:

1. All company-owned assets and devices are returned, and Taufolio data on personal devices is deleted.
2. The person is removed from all critical systems, and access is revoked immediately and no later than the end of the last working day. Revocation covers GitHub, Vercel, Supabase, Clerk, Stripe, Resend, PostHog, Sentry, AI provider consoles and any other system recorded in the access register.
3. Personal access tokens and API keys created by or known to the person are revoked, and shared credentials are rotated.
4. Each revocation is checked against the provider's member list and recorded in the access register with the date.
5. If access to an account must be retained, the credentials of that account are changed and the justification is recorded.

On a change of role, the Information Security Officer reviews and adjusts access under the Access Control Procedure.

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 onboarding and offboarding records and feedback to the policy owner. Any staff member found to have violated this procedure 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.

6. Responsibilities

The Information Security Officer is responsible for approving and reviewing this procedure and for carrying out its steps. Staff members are responsible for applying the relevant sections 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 HR Security 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