



PROCEDURE · ACCESS CONTROL

Access Control 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. Access control procedure

4. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

This procedure sets out how user access to Taufolio's assets and information systems is managed and controlled, in line with the Access Control Policy.

2. Scope

This procedure applies to all users and administrators with access to any critical system at Taufolio.

3. Access control procedure

3.1 Requirements for access control

- The Information Security Officer maintains the **access register**, held in Taufolio's internal documentation. It lists every critical system, the roles that may access it, each account with access, the person it belongs to, the privilege level, the MFA status and the date of the last review.
- Critical systems include Vercel, Supabase, GitHub, Clerk, Stripe, Resend, PostHog, Sentry, the AI provider consoles and the brokerage integrations.
- Where a provider offers an audit log or a member list (GitHub, Vercel, Supabase, Clerk, Stripe), the Information Security Officer uses it as the source of truth for who holds access, and compares it with the register. Where a system offers no such facility, its accounts are recorded in the register by hand.
- The Information Security Officer ensures that the roles that may obtain access to each critical system are defined in the register.

3.2 Access provisioning

1. Access is initiated only after the staff member has signed the terms of engagement, including the information security obligations, and has accepted the Acceptable Use Policy.
2. By default, new staff members receive only the systems configured for all staff, such as email and internal messaging.
3. Access to other systems is granted by the administrator of that system according to the role matrix, on a request approved by the Information Security Officer. The request, the approver, the date and the privilege level are entered in the access register.
4. Each account created in a system must be linked to the staff member's company email address so that users are identified and can be tracked.
5. MFA must be enabled on the account before access to a production system is used.
6. Access for third parties (consultants, auditors, vendors) must be approved by the Information Security Officer, limited in scope and in time, and disabled by the administrator as soon as the need ends. The end date is entered in the register.

7. Accounts that appear in a provider member list but not in the register are treated as unauthorized. The Information Security Officer investigates each one and either records it with a justification or removes it.

3.3 Management of privileged access rights

- System administrators must follow the principle of least privilege when granting access.
- During access reviews, the Information Security Officer reviews the privileges assigned to each user together with the administrators of the individual systems.
- Customer data must remain reachable from production only through server-side code and the secret server key. Decrypted brokerage credentials must not be exposed in any administrative tool, and no administrator is granted a way to read them.
- Production secrets and keys are held only in the hosting provider's secret store. Access to them is limited to the Information Security Officer and the automated deployment.

3.4 Management of secret authentication information

- MFA and, where available, single sign-on must be enabled on every critical system.
- The Information Security Officer checks the MFA status of every account in the register at each access review and whenever a new account is added. An account without MFA is suspended until MFA is enabled.
- Passwords are stored only in an approved password manager. Where a system supports only password log-in, the Information Security Officer records in the register how secure password handling is enforced.

3.5 Review of access rights

- The Information Security Officer reviews access to all production systems at least once every quarter, with help from the administrators of each system. Non-production systems are reviewed at least annually.
- Each review compares the provider member lists and audit logs with the access register, confirms that every account is still needed, and checks the privileges of each user for segregation of duties.
- The date, the reviewer, the findings and every corrective action are recorded in the access register. Corrective actions are completed immediately, and the register is updated when they are done.

3.6 Removal or adjustment of access rights

1. When a staff member leaves, or when their role changes, the Information Security Officer is notified at once.
2. On termination, access to all critical systems is revoked immediately, and no later than the end of the last working day. Provider accounts, repository membership and personal access tokens are removed or revoked, and shared credentials and keys known to the person are rotated.
3. Company assets and devices are returned, as set out in the HR Security Procedure.

4. On a change of role, the Information Security Officer adjusts access so that it matches the new role and updates the role matrix.
5. If a person's access to an account must be retained for a business reason, the credentials of that account are changed and the justification is recorded in the register.
6. Each revocation is confirmed against the provider's member list and recorded in the register with the date.

3.7 User responsibilities

- Users must follow the access control policy and this procedure.
- Users must keep passwords and MFA devices confidential, and change a password whenever compromise is suspected.
- Sharing of passwords or authentication information must be reported to the Information Security Officer by email at once.
- Users must not leave a system unattended while logged on, and must lock the screen even when stepping away briefly.

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 access reviews, provider audit logs and feedback to the policy owner. Any staff member found to be in violation 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, for keeping the access register and for carrying out the reviews. System administrators and 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 Access Control 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