



POLICY · ACCESS CONTROL

Access Control 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. Access control rules

5. Document security classification

6. Non-compliance

7. Responsibilities

8. Schedule

9. Version history

1. Objective

The objective of this policy is to provide a framework that ensures access to Taufolio assets is granted in a controlled manner, based on business and information security requirements.

The framework establishes the access management controls needed to protect Taufolio assets, and the data of its users, from threats arising from unauthorized access. This matters most for the credentials and portfolio data that users entrust to Taufolio.

2. Scope

This policy applies to the systems that have a significant effect on Taufolio's ability to deliver its service and to safeguard information. These include, but are not limited to:

- the production application and infrastructure on Vercel;
- the production database and file storage on Supabase;
- the authentication service (Clerk) and the payment service (Stripe);
- the source code repository on GitHub and the CI and release tooling around it;
- email, analytics, monitoring and AI provider consoles that can reach Taufolio data;
- brokerage integrations, including SnapTrade and the direct tastytrade and Interactive Brokers connectors.

3. Policy statement

Centralized, documented access control ensures that the right staff members reach the right data and systems at the right level. The principle of least privilege guides every access decision. The controls apply to information and processing systems at the application and operating system layers, including networks and network services.

The confidentiality, integrity and availability of information held in Taufolio's systems must be assured by allowing only authorized users to access specific information assets, and only as needed for their work.

4. Access control rules

4.1 Requirement for access control

- Every organization holds information and assets that must be protected from unauthorized use.
- The Information Security Officer must identify and document the critical systems that host services or sensitive data within the scope of this policy, and keep that list up to date in the access register.
- The list of critical systems must be reviewed whenever a new provider, integration or environment is introduced.

4.2 Access management

4.2.1 Access provisioning

Access to Taufolio systems must be provided according to these principles:

- **Need to know.** Users and services are granted access only to systems necessary for their role.
- **Least privilege.** Users and services receive the minimum privileges needed to fulfill their role.
- **Separation of duties.** Where practicable, responsibility for critical actions is distributed so that a single individual cannot subvert a process. Where the team is too small for full separation, compensating controls such as code review, provider audit logs and post-change checks must be applied.

The minimum access control requirements must be met using one or both of the following methods.

Role-based access control. Access is restricted according to the role of the staff member rather than the individual.

- The roles that may access each critical system must be identified and documented.
- Access is granted by role. The ability to grant access to a system is restricted to the administrators of that system.
- Any access outside the defined role matrix requires a documented business justification.

Request-based access control. Access is granted through a documented request and approval.

- Requests for accounts and access privileges must be documented and approved by the Information Security Officer. The authorization record must be retained for as long as business, contractual and legal requirements demand.
- A request must state the specific access needed.
- Staff members must accept the Acceptable Use Policy before being granted access to systems that contain customer data.
- Access outside the default for a role must be limited to the minimum level required for the intended business operation.

4.2.2 Management of privileged access rights

- Access is considered necessary only when a staff member cannot perform a function without it. If an action can be performed without the requested access, the access is not necessary.
- Administrative access to production systems (Vercel, Supabase, GitHub organization settings, Clerk, Stripe and AI provider consoles) must be limited to named accounts held by the Information Security Officer and to staff members who need it. Shared administrator accounts must not be used.
- Taufolio's administrative tooling must never expose decrypted brokerage credentials. Staff members cannot view them in any administrative tool.

- The production database must be accessed only by server-side code using a secret server key held in the hosting provider's secret store. Anonymous and publishable database keys must not be enabled, and no browser or mobile client may reach the database directly.
- Direct database administration must be restricted to named administrator accounts protected by MFA, over SSL.
- Least privilege protects Taufolio and its users from unauthorized access and configuration changes, and limits the damage if an account is compromised.

4.2.3 Management of passwords and secret authentication information

Reliance on passwords must be minimized.

- Multi-factor authentication (MFA) is mandatory for all staff accounts on production systems, including GitHub, Vercel, Supabase, Clerk, Stripe and email. MFA adds a barrier even if a password is compromised.
- Single sign-on or the provider's federated login should be used wherever it is available.
- Where a password is the only mechanism, it must be unique to that account, at least 12 characters long, and generated and stored in an approved password manager. Passphrases of 16 or more characters are encouraged.
- Passwords must never be reused from personal accounts, and must be changed immediately if compromise is suspected. Routine periodic expiry is not required when MFA is in place.
- Passwords and secrets stored in Taufolio systems must be hashed, encrypted or masked. Application secrets must be held only in the hosting provider's secret store, as set out in the Encryption Policy.
- Passwords must never be shared with anyone, including colleagues.
- Account lockout should be configured after 5 failed log-in attempts, and repeated failures should be monitored.

4.2.4 Review of access rights

- User accounts and their rights must be reconciled periodically. Reviews of production systems must take place at least quarterly, and of other systems at least annually. Each review is recorded in the access register.
- A review must include the privileges assigned to each user, not only the existence of the account.
- Irregularities must be removed, disabled or corrected immediately.

4.2.5 Removal or adjustment of access rights

- Termination of employment or engagement, or a change of role, triggers revocation or adjustment of access.
- On a change of role, access must be adjusted so that the person holds no more rights than the new role requires.

- Access of departing staff members, including contractors, must be revoked immediately, and in any case no later than the end of the last working day. This includes provider accounts, repository membership, tokens and API keys they created or knew, and any shared credentials, which must be rotated.

4.2.6 Secure log-on

- A failed log-in must not reveal which part of the credentials was wrong.
- The number of unsuccessful log-on attempts must be limited, and passwords must not be displayed while typed.
- MFA must be used on all critical systems, as set out in 4.2.3.
- Inactive application and administration sessions must be closed after a defined period of inactivity where the platform allows, and re-authentication may be required at intervals.

4.2.7 Access monitoring

- Logging must be enabled on all production infrastructure so that user accountability is maintained. Provider audit logs (GitHub, Vercel, Supabase, Clerk, Stripe) must be kept enabled and used when investigating any incident.
- Unusual access, such as repeated failed log-ins or administrator actions that cannot be explained, must be reported to the Information Security Officer.

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 audit log reviews, access reviews, code review and feedback to the policy owner. Non-compliance may result in disciplinary action, up to and including termination of employment or of the contractual agreement, and may lead to legal action.

7. Responsibilities

The Information Security Officer is responsible for implementing and maintaining this policy and for ensuring that staff members understand their responsibilities. All staff members must comply with this policy and with any additional access control measures.

8. Schedule

This document is reviewed at least annually and whenever a significant change occurs in Taufolio's systems or organization.

End of Access Control 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