



POLICY · PEOPLE

Acceptable Use 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. Separation of concerns

5. Security of critical data

6. Unacceptable use

7. Document security classification

8. Non-compliance

9. Responsibilities

10. Schedule

11. Version history

1. Objective

Taufolio is committed to safeguarding the data processed by its staff, software and services. Users, partners and brokerage providers depend on Taufolio to protect the data in its care, including portfolio data and the credentials users grant for read-only brokerage connections. Each staff member must therefore understand how to use Taufolio's systems responsibly.

2. Scope

This policy applies to all staff members, meaning employees, contractors, consultants, temporary workers and anyone else who interacts with Taufolio systems. Everyone covered is responsible for using electronic devices, data and network resources with good judgment and in line with policies, standards, local laws and regulations. The policy applies to:

- any device used for Taufolio work, whether issued by Taufolio or personally owned, that stores or accesses Taufolio data;
- Taufolio's systems on the internet, including servers, software, storage and network accounts;
- Taufolio-administered accounts with third-party services that provide email, storage, hosting, source control, databases, payments, analytics, AI models, APIs or business systems, regardless of whether they are accessed from devices owned by Taufolio, by the staff member or by a third party.

3. Policy statement

Taufolio has a culture of trust and integrity. This policy reinforces that trust by ensuring that we can depend on each other to protect the assets of our users, partners, staff and company.

Security is a shared effort and needs the cooperation of every staff member who works with Taufolio systems. Individuals must take precautions to use systems appropriately and must not deliberately or accidentally perform destructive or illegal actions.

4. Separation of concerns

Accounts and devices used for Taufolio work are not personal property. Their use for personal reasons should be limited, and personal accounts and files should be kept separate from Taufolio accounts and data.

5. Security of critical data

- All Taufolio data stored on computing and storage devices remains the property of Taufolio, whether the device is owned by Taufolio, by the staff member or by a third party.
- Critical data must be handled and secured according to the Data Classification Policy.

- Theft, loss or unauthorized disclosure of critical data must be reported promptly to the Information Security Officer by email to support@taufolio.com.
- Critical data may be accessed, used or shared only to the extent authorized and necessary for the staff member's responsibilities.
- Brokerage credentials and other customer secrets must never be copied out of the systems that hold them, pasted into chats, tickets, documents, logs or AI tools, or requested from a user. Staff members cannot view them in administrative tools and must not try to bypass this.
- Devices used for Taufolio work must use full-disk encryption, a screen lock and current security updates, and accounts on production systems must use MFA.
- Staff members must use good judgment in reasonable personal use of Taufolio systems and consult the Information Security Officer when unsure.
- Taufolio may audit any system at any time to verify compliance with this policy, and authorized individuals may monitor equipment, systems and network use.

6. Unacceptable use

Staff members must not use Taufolio-managed resources for activities that are illegal or prohibited under applicable law, whatever the circumstances.

6.1 Unacceptable system and network activities

- Violating the rights of any person or company protected by copyright, trade secret, patent or similar intellectual property laws or regulations.
- Copying, distributing or using copyrighted material without authorization.
- Exporting software, technical information, encryption software or technology in violation of international or national export control laws.
- Deliberately introducing malicious programs into Taufolio systems or any device managed for Taufolio.
- Deliberately misusing Taufolio systems or devices, for example for cryptocurrency mining or botnet control.
- Sharing credentials for any Taufolio system or third-party service used by Taufolio, or letting others use your account or device. This does not apply to single sign-on or similar technologies, which are approved.
- Using a Taufolio asset to obtain or transmit material that constitutes harassment or creates a hostile working environment.
- Making fraudulent offers of products, items or services from any Taufolio account.
- Deliberately accessing data, or logging into a computer or account, that the staff member is not authorized to access, or disrupting network communication, processing or access.
- Intercepting data not intended for the staff member's own device with network monitoring tools, except when troubleshooting for the benefit of Taufolio.

- Circumventing user authentication or the security of any host, network or account used by Taufolio.
- Tunneling between network segments or security zones, except when troubleshooting for the benefit of Taufolio and its users.
- Sending production data, personal data or portfolio contents to a tool or AI service that is not an approved Taufolio subprocessor.

6.2 Unacceptable email and communications activities

- Forwarding confidential business emails or documents to personal external email addresses.

Taufolio may retrieve messages from archives and servers without prior notice where there is sufficient reason. Any such investigation must be carried out with the knowledge of the Information Security Officer and, where needed, legal counsel.

6.3 Return of Taufolio-owned assets

All Taufolio-owned computing resources and all Taufolio data must be returned or securely deleted when a staff member leaves, as set out in the HR Security Policy.

7. Document security classification

Public. This document is published in the Taufolio Trust Center. See the Data Classification Policy for the classification levels.

8. Non-compliance

Compliance with this policy is verified through audits, provider audit logs, code review 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.

9. 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.

10. Schedule

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

End of Acceptable Use Policy. For the version history, see the next page.

11. 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