



POLICY · INFRASTRUCTURE AND OPERATIONS

Physical and Environmental 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. Physical security

5. Working remotely

6. Document security classification

7. Non-compliance

8. Responsibilities

9. Schedule

10. Version history

1. Objective

The purpose of this policy is to establish the guidelines by which physical and environmental security is managed for the systems within the scope of Taufolio's information security program.

2. Scope

This policy applies to all processes and operations at Taufolio within the scope of the information security program, and to every staff member (employees and contractors), wherever they work.

3. Policy statement

Taufolio is a remote-first, cloud-native company. It operates no data center and no server room, and no production server or customer data is hosted on premises. The physical and environmental security of production infrastructure is inherited from the independently audited data centers of Taufolio's cloud providers. Taufolio's own responsibility is the physical security of the places where staff members work and the devices they use: home and other remote workspaces, laptops and mobile devices. Staff members must keep their devices secure, protect the confidentiality of customer data and follow Taufolio's information security policies wherever they work.

4. Physical security

4.1 Production infrastructure

- All production infrastructure, including the application hosting, the database and the file storage, is secured and managed by Taufolio's cloud providers in their own data centers. Taufolio relies on the physical security measures of these providers to protect the security, availability and confidentiality of production systems.
- Because no production server or customer data is hosted in places Taufolio controls, the risk of physical access to production infrastructure is transferred to those providers. Taufolio must review that reliance as set out in the Physical and Environmental Security Procedure and the Vendor Management Policy.

4.2 Workspaces

The physical security of the places where staff members work remains essential. The following rules apply to home offices, shared workspaces and any other location:

- **Visitors:** a staff member is responsible for the actions of any visitor they allow into their workspace and must keep visitors away from screens and devices that show Taufolio data. Do not allow people you do not know or trust to work near Taufolio devices or data.

- **Clean desk:** no classified customer data, keys or passwords may be written on whiteboards, unattended notepads or sticky notes.
- **Printing:** printing customer data, keys, passwords or other classified information is prohibited.
- **Removable media:** removable media must not be used to transfer sensitive customer data on devices used for Taufolio work.
- **Shoulder surfing:** when working in a public place such as a cafe, train or airport, staff members must be aware of shoulder surfing, and must avoid showing or discussing Taufolio data where others can see or hear it.
- **Local laws:** staff members must comply with local laws that apply to their workspace, for example on fire safety.

5. Working remotely

Staff members who work remotely must follow these rules:

- The security of the device used for work is the staff member's responsibility. The device must be in their presence, with the screen locked, or stored securely.
- Any equipment used for Taufolio work, whether supplied by Taufolio or personally owned, must follow Taufolio's endpoint protection and encryption standards, as set out in the Endpoint Security Policy.
- The confidentiality, security and privacy of customer data must be protected, so that unauthorized people cannot view, overhear or otherwise access it.
- Home and public networks must be treated as untrusted. Access to production systems must use accounts protected by multi-factor authentication.
- All remote work must be performed in a manner consistent with Taufolio's information security policies.

6. Document security classification

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

7. Non-compliance

Compliance with this policy is verified through periodic internal reviews, confirmation by staff members 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 their contractual agreement. The action depends on the extent, intent and consequences of the violation.

8. 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.

9. Schedule

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

End of Physical and Environmental Security Policy. For the version history, see the next page.

10. 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