



PROCEDURE · INFRASTRUCTURE AND OPERATIONS

Physical and Environmental 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. Process responsibilities

4. Physical security requirements

5. Requirements for physical assets

6. Clear desk and clear screen

7. Document security classification

8. Non-compliance

9. Responsibilities

10. Schedule

11. Version history

1. Objective

Taufolio's information security program protects the organization's sensitive information from unauthorized access, loss and inaccuracy. This procedure sets out the steps that prevent unauthorized physical access, avoid damage to assets, and prevent interference with Taufolio's information and information processing facilities.

2. Scope

This procedure covers the production environment facilities provided by Taufolio's cloud providers, their supporting functions, and the physical assets used by staff members, such as laptops and mobile devices. Taufolio operates no data center and no server room.

3. Process responsibilities

3.1 Information Security Officer

The Information Security Officer is responsible for:

- reviewing the device security status checks;
- reviewing provider assurance as set out in section 4;
- allocating and deallocating devices and access, and recording both in the asset inventory;
- training staff members in the use of physical assets such as laptops;
- ensuring that information assets are returned and access to systems is removed when a staff member leaves.

3.2 Staff members

Each staff member is responsible for protecting the assets in their care, for locking or securing them as set out in sections 5 and 6, and for reporting loss or theft immediately.

4. Physical security requirements

- Taufolio is a software as a service (SaaS) company. Its production infrastructure is hosted by third-party cloud providers whose data centers are independently audited.
- The Information Security Officer must review the agreements with these providers at least annually, with legal advice where needed, and must collect and review the providers' current published security assurance (such as security reports and audit summaries) to confirm that each provider can protect the confidentiality, integrity and availability of Taufolio's data. Findings must be recorded, and a provider that no longer meets Taufolio's needs must be handled under the Vendor Management Policy.

- Staff workspaces are outside the production environment, because no production server or customer data is hosted there. They are covered by the Physical and Environmental Security Policy and by the endpoint rules.

5. Requirements for physical assets

- Each user is responsible for protecting the assets in their care and must give their security due importance.
- The Information Security Officer must ensure that staff members who use assets such as laptops understand the information security requirements for protecting unattended equipment, and their own responsibilities for applying them, through onboarding and periodic security awareness training, in line with the Asset Management Policy and the Human Resources Security Policy.
- Staff members must not leave equipment unattended. They must end active sessions when finished unless the session can be secured by an appropriate locking mechanism. Examples are a password-protected screen lock, logging out of applications that are no longer needed, and protecting laptops and mobile devices with a password or biometric lock.

6. Clear desk and clear screen

The clear desk rules apply to paper (hardcopy) and to laptops, so that unauthorized people cannot reach Taufolio information. Paper should be avoided, and where it is unavoidable, the following apply.

6.1 Clear desk

- Confidential paper assets, such as customer, project or product development documents, must not be left unattended where unauthorized people could access them.
- Passwords must not be written down on paper. They must be kept in a password manager.
- Workspaces must be left clear before leaving them for a longer period.
- An incident involving loss of information must be reported immediately to the Information Security Officer, and handled under the Incident Management Procedure.

6.2 Clear screen

- Users must lock their computers when leaving their desks and log off when leaving for an extended period. This protects the screen contents from prying eyes and the computer from unauthorized access.
- Privacy screens should be used where the risk of shoulder surfing is high.
- Users must not keep files or shortcuts holding sensitive data on the desktop.
- Users must empty the recycle bin regularly.

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 procedure is verified through periodic internal reviews, confirmation by staff members 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 their 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 procedure and the related policies. Staff members are responsible for applying the relevant sections of this procedure 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 Physical and Environmental Security Procedure. For the version history, see the next page.

11. 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