



POLICY · DATA PROTECTION AND PRIVACY

Media Disposal 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. Document security classification

5. Non-compliance

6. Responsibilities

7. Schedule

8. Version history

1. Objective

Secure disposal of electronic and physical media adds a layer of protection that prevents critical data from being exposed to unauthorized individuals. This policy aims to reduce the risk of unauthorized data recovery. It shows users, staff members and partners that Taufolio protects their data even after it has served its purpose.

2. Scope

This policy applies to all devices, equipment and media that process, store, transmit or give access to Taufolio data. In particular it applies to laptops, workstations, mobile devices, external drives and removable media used for Taufolio work that are being permanently decommissioned, sold, handed on or returned, including personally owned devices that have held Taufolio data. It also covers paper printouts of Taufolio information.

Taufolio runs on managed cloud services (hosting, database, file storage). Physical media in those services belongs to the providers, which are responsible for their disposal under their own security programs. For data held there, deletion follows the Data Retention and Deletion Policy.

3. Policy statement

Before a device or medium leaves Taufolio's control, the data on it must be rendered unrecoverable. The method depends on the classification of the data it held, as defined in the Data Classification Policy.

3.1 Methods

1. **Encryption.** The entire disk must be encrypted with a robust algorithm and a strong passphrase. Staff laptops must use full-disk encryption from the start, so that this method is already in place for any device.
2. **Secure erasure.** All information must be erased with software that securely overwrites it or, for solid-state drives and phones, cryptographically erases it or performs a factory reset after encryption. A simple delete or quick format is not sufficient.
3. **Physical destruction.** The device or medium is destroyed, for example by shredding or incineration, by a method that makes recovery impossible.

3.2 Required methods by classification

- Media that held **Restricted** data (customer brokerage credentials, API keys, master keys, production secrets) must be disposed of using all three methods where physical destruction is possible, or by encryption followed by secure erasure for devices that are to be reused. Any credentials that were ever stored on the device must also be revoked or rotated.

- Media that held **Confidential** data must be disposed of using at least encryption followed by secure erasure.
- Media that held only **Internal** or **Public** data require at least one method.

3.3 Other requirements

- Before disposal, the staff member must confirm that Taufolio data has been backed up or migrated where needed, and that the device is signed out of Taufolio accounts and removed from password managers, authentication apps and provider sessions.
- The Information Security Officer must update the asset inventory to record the disposal: the asset, the date, the data classification, the method used and who performed it. If a third-party disposal service is used, it must provide written confirmation of destruction.
- Paper containing Confidential or Restricted information must be shredded.
- Lost or stolen media is not a disposal but an incident: it must be reported immediately under the Incident Management Policy so that access can be revoked.

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 policy is verified through asset inventory reviews, periodic internal reviews 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.

6. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures, and for maintaining the disposal records. Staff members are responsible for applying the relevant sections of this policy 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 Media Disposal Policy. For the version history, see the next page.

8. 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