



POLICY · DATA PROTECTION AND PRIVACY

Encryption 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. Encryption guidelines

5. Approved algorithms

6. Document security classification

7. Non-compliance

8. Responsibilities

9. Schedule

10. Version history

1. Objective

Encryption encodes data so that it stays unreadable to anyone who is not authorized to see it. By encrypting data at rest and in transit, Taufolio protects personal, proprietary and critical data, and secures the communication between users' browsers, Taufolio's servers and the third-party services Taufolio connects to on a user's behalf.

This policy sets the rules for encrypting data at Taufolio, with particular attention to the most sensitive data Taufolio holds: the credentials a user grants Taufolio to read their brokerage account.

2. Scope

This policy applies to every system and network that stores or transfers Taufolio data, including:

- the production application hosted on Vercel and its server-side code;
- the production database and file storage on Supabase (EU, Ireland);
- cloud services that process Taufolio data on its behalf (subprocessors);
- endpoints (laptops and mobile devices) used by staff members;
- integrations with brokerage providers, including SnapTrade and the direct tastytrade and Interactive Brokers connectors.

3. Policy statement

All Taufolio data must be encrypted at rest and in transit. Data at rest is protected by provider-managed encryption of the underlying storage and, for customer credentials, by an additional layer of application-level encryption whose keys are held outside the database. Data in transit is protected by TLS using certificates from trusted public authorities. Passwords and cryptographic keys must be stored only in purpose-built secret stores. Staff members must not design their own cryptographic algorithms.

4. Encryption guidelines

4.1 Encryption at rest

- Data at rest is data that is physically stored and not moving between locations, for example in a database, in object storage, in backups or on a laptop.
- Taufolio's production database and file storage run on a managed platform (Supabase) that encrypts the underlying storage and its backups with AES-256. The provider manages these storage keys.
- Staff laptops must use full-disk encryption, as set out in the Endpoint Security Policy.
- Exports of personal data (for example a user's data-access request) must be stored only in encrypted storage and deleted once delivered.

4.2 Encryption in transit

- Data in transit is data moving from one location to another, for example over the internet or between cloud services.
- Every connection to taufolio.com and to Taufolio's APIs must use HTTPS with TLS 1.2 or higher. HTTP Strict Transport Security (HSTS) is enabled for taufolio.com.
- Connections from Taufolio's servers to the database, to subprocessors and to brokerage APIs must use TLS.
- All public-facing Taufolio properties must use certificates issued by a known, trusted certificate authority, renewed automatically before expiry.

4.3 Customer credentials and brokerage connections

When a user connects a brokerage account, Taufolio may hold OAuth client identifiers and client secrets, OAuth access and refresh tokens, API keys or a provider-issued user secret. These credentials are protected as follows:

1. **Application-layer encryption before storage.** Every credential is encrypted by Taufolio's server-side code before it is written to the database, using AES-256-GCM (authenticated encryption). Each record has its own random 128-bit salt and 96-bit initialization vector.
2. **Per-user, per-provider keys.** The encryption key for each record is derived with HKDF-SHA-256 from a master key and bound to the user's identifier and the provider's name. A ciphertext therefore cannot be decrypted for another user or replayed against another provider, and the GCM authentication tag detects any modification.
3. **The master key never lives in the database.** The master key is held only in the hosting provider's encrypted secret store, marked as sensitive so it cannot be read back from the dashboard, and is available only to server-side code. A complete copy of the database, including its backups, does not reveal any customer credential.
4. **A dedicated, server-only table.** Credentials are stored only in a dedicated secrets table. Row Level Security is enabled and forced on it with no access policies, and every privilege is revoked from the public API roles, so the table cannot be read, changed or emptied through the database's public API.
5. **No client-side database access.** No browser or mobile client talks to the database. Taufolio does not use anonymous or publishable database keys; the legacy anonymous key and all publishable keys are disabled. Only server-side code holding the secret server key can reach the data.
6. **Never logged, never displayed.** Credentials must never be written to application logs, error reports, analytics events or AI model prompts, and are never returned to the browser after they are saved. Decryption happens only in memory, in the server process that calls the broker, and staff members cannot view decrypted credentials in any administrative tool.
7. **Read-only scopes.** Taufolio requests only read-only access (accounts, positions, balances and transactions). It must never request trading, order-placement, withdrawal or transfer permissions.
8. **Deletion on disconnect.** When a user disconnects a brokerage account or deletes their Taufolio account, the encrypted credentials are hard-deleted immediately.

4.4 Uploaded broker statements and screenshots

Users can import a portfolio by uploading a broker statement (CSV, XLSX or XML) or a screenshot. These files are Confidential data and are protected as follows:

1. **Encrypted in transit and at rest.** Files are uploaded over TLS to Taufolio's server and stored in a dedicated, private object store used only for portfolio imports. The storage provider encrypts the stored objects at rest.
2. **No public address.** The store is private: no file in it has a public URL, and every read must be authenticated with an access token that exists only in the hosting provider's encrypted secret store and is available only to server-side code. A file cannot be fetched from the internet, by another user, or from the browser of the user who uploaded it.
3. **Random, non-descriptive storage paths.** Each file is stored under random identifiers of the workspace, the import and the file. The original file name and the user's identity do not appear in the storage path.
4. **Isolated processing.** Files are read by Taufolio's server. When a file format is new and a parser has to be generated for it, that parser runs in an isolated sandbox (a dedicated microVM) with no network access, no environment variables, no secrets and no database connection, under a hard time limit, and is destroyed after the run.
5. **Restricted staff access.** A retained file can be opened only by the platform administrator, through an administrator-only server route that streams it without ever creating a link, to resolve a support case or a parsing error. No other staff member, partner or service has access.
6. **Short retention and deletion.** Statement files are deleted automatically 30 days after upload, or after up to 365 days when the user agreed to let Taufolio keep the file to improve statement parsing. Screenshots are deleted right after a successful analysis, or after 7 days at the latest if the analysis failed. Cancelling an import deletes its files immediately, and deleting the account deletes all of them. An automated job enforces these limits.

4.5 Passwords

- User passwords are handled by Taufolio's authentication provider (Clerk), which stores them as salted, adaptive hashes. Taufolio's own systems never receive or store user passwords.
- Staff passwords and shared service credentials must be stored only in an approved password manager or in the hosting provider's secret store, never in source code, documents or chat messages.

4.6 Cryptographic keys

- Cryptographic keys must be generated with a cryptographically secure random number generator and must be at least 256 bits long for symmetric encryption.
- Keys must be stored in a way that prevents loss, theft or disclosure: in the hosting provider's secret store or a managed key service, never in the repository and never in the database they protect.

- The master key for customer credentials must be rotated at least annually, immediately if compromise is suspected, and whenever a person with access to it leaves Taufolio. During rotation, the previous key remains available for decryption only until every secret has been re-encrypted under the new key, after which it must be destroyed.
- Access to production keys is limited to the Information Security Officer and to the automated deployment that injects them into the runtime.

4.7 Do not roll your own cryptography

Staff members must use well-established, publicly reviewed algorithms and the standard libraries of the platform (for example the Node.js crypto module). Anyone who believes they have a case for a custom cryptographic design must contact the Information Security Officer, who will help find a standard alternative.

5. Approved algorithms

Purpose	Minimum standard
Symmetric encryption	AES-256-GCM
Key derivation	HKDF-SHA-256
Hashing for integrity and signatures (HMAC)	SHA-256 or stronger
Transport	TLS 1.2 or higher, TLS 1.3 preferred
Password storage	Adaptive salted hashing managed by the authentication provider

Algorithms that are deprecated or broken (for example DES, 3DES, RC4, MD5 and SHA-1 for security purposes) must not be used.

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 code review, automated tests, provider audit logs, 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.

8. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and the related procedures, and for managing production keys. 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 Encryption 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