

Encryptio — User manual

Web and browser extension · updated 2026-09-24

A practical guide to the current product.

Contents

- 1. What Encryptio is
- 2. Registration and sign-in
- 3. Master password and auto-lock
- 4. Vault: passwords and notes
- 5. Recovery key
- 6. Two-factor authentication (2FA)
- 7. One-time secure share (Premium)
- 8. Digital Legacy (Premium)
- 9. Plans and pricing
- 10. Browser extension
- 11. Public tools
- 12. Profile and preferences
- 13. Support and good practice
- 14. Server backups (security policy)

1. What Encryptio is

Encryptio is a zero-knowledge password and secret-note manager: encryption happens on your device. The server stores only an already-locked vault and cannot read it.

Use the web app in any modern browser. On Chrome, Firefox, and Edge you can also install the extension (unlock, Fill, Open from the vault). Safari uses the website — there is no store extension. There are no native phone apps: on a phone, open the same site in the browser.

Without an account you can use the public Tools (password generator and Encrypt text). The vault requires registration.

2. Registration and sign-in

Registration: enter an email you control and accept Terms and Privacy. You receive a one-time link (valid 30 minutes). Then choose a master password (at least 12 characters) and accept Terms and Privacy again — only then is the vault created. There is no account without a vault.

Right after creation Encryptio offers to create a recovery key (you can skip and do it later in Profile → Security).

Sign-in: email + master password. If 2FA is on, also enter an authenticator or backup code.

Session and vault are separate. The session cookie may last several hours even if you close the browser — you still look “signed in”. The vault key lives only in memory: after idle lock, a reload, or closing the browser you must enter the master password again on Unlock.

In Profile (vault unlocked) you can change the account email: re-enter the master password and confirm the new address with a one-time link. The vault is untouched; other devices must sign in again.

Deleting the account (Profile) requires a session, matching email, and the confirmation word

DELETE. It permanently drops the user row and ciphertext on the server. Export a local backup first if you need a copy.

3. Master password and auto-lock

The master password never leaves your device. Encryptio cannot reset it or open your data without it (or without a recovery key).

The browser derives two materials: the vault key (in memory only while unlocked) and an auth secret used only to prove sign-in to the server.

After inactivity (default 15 minutes, changeable in Profile → Preferences; 0 = never) the vault locks by itself: the key leaves memory and you must enter the master password again. Staying signed in is not enough.

In Profile you can also choose where to land after unlock (combined list, passwords only, or notes only).

4. Vault: passwords and notes

After unlock you get a combined list under Vault, passwords under Vault → Passwords, and notes under Vault → Secret notes (or the menu shortcuts).

Each password can have title, username, password, site URL, and tags. Secret notes are long text (licenses, codes, private notes) with title and tags.

You can search, sort, and paginate. On passwords you can filter at-risk items (weak, reused, outdated) and open the edit form from a risk badge.

JSON or CSV import and export run only on your computer with the vault unlocked. There is no server-side export. The export file is plaintext: keep it somewhere safe and delete it when you no longer need it. You can also import older Encryptio or common vault files, always in the browser.

With the extension installed, clicking a password URL opens the site and can fill the login fields. Without the extension the link still opens in a new tab.

Starter (free): up to 15 passwords and 15 notes. Premium removes those limits. If you return to Starter over the limit, the oldest 15 per type stay editable; newer excess items are view and delete only until you trim the list or go Premium again. Local export still includes everything.

5. Recovery key

The recovery key is your plan B if you forget the master password. It is offered after registration and you can create (or recreate) it in Profile → Security.

It is shown once: copy or print it and keep it offline somewhere safe. Encryptio will not email it again and does not offer a JSON download of the key.

To use it: Forgot password → open the email link (valid 24 hours) → enter the recovery key and choose a new master password. Without a recovery key, losing the master password means the data stays sealed forever — including for us.

After recovery or a master-password change, Digital Legacy must be set up again (new keys for contacts).

6. Two-factor authentication (2FA)

Optional. It protects account sign-in only and does not replace the master password for vault unlock. Enable it in Profile, scan the QR or enter the secret in an authenticator app, then store the one-time backup codes shown once.

7. One-time secure share (Premium)

From Vault → Share securely (or My shares) you can create a one-time link: text or one vault item is encrypted on your device; the key stays in the URL fragment (after #). Encryptio stores ciphertext only.

Whoever opens the link can use it once (or until it expires). Then the share is gone. No Encryptio account is required to open the link.

Available with Premium or an active trial. Do not confuse it with Digital Legacy (long-term emergency access) or Encrypt text (public tool, not linked to the vault).

8. Digital Legacy (Premium)

In Profile → Digital Legacy you can name up to five trusted contacts, ordered by priority, for emergency read-only access.

When you add a contact, the browser creates a Legacy access key and a wrap of the vault key. The key is shown once: give it to the contact out of band (print or a secure channel). Encryptio does not email it.

The contact requests access from the public page `/legacy/request`. A waiting period starts (configurable); you can cancel anytime from Profile.

After grant they get a link: they must confirm (anti-prefetch) and enter the Legacy key. They open a timed read-only view — no edits, export, or new shares.

With multiple contacts, if the window expires without the delegate opening access, the system moves to the next contact (escalation).

Optional: inactivity trigger. After the set idle days you get a grace warning; if you do not become active again, the top-priority contact may receive the grant. Still zero-knowledge: Encryptio never holds the vault key in the clear or in escrow.

Without Premium (or an active trial) you cannot configure Digital Legacy; contact requests will not start.

9. Plans and pricing

Starter: free (15 + 15 limits). Premium: €3.99/month or €2.79/month billed yearly (see Pricing for the annual total). One-time 30-day Premium trial, no card.

Premium removes item limits and unlocks one-time share and Digital Legacy.

Paid subscriptions use PayPal (server-side checkout, no PayPal JS SDK on the page). Details and what happens if you return to Starter: Pricing and Profile → Plan.

10. Browser extension

Chrome, Firefox, and Edge: install Encryptio from the site's Extension page (or the linked stores).

Do not use the old Flask product's extension.

From the popup: unlock with the master password (and 2FA at login if enabled), search including tags, sort, Fill on the open tab, or Open to go to the site and fill.

From the web vault, with the extension active, clicking the password URL opens and fills. The key stays in the service worker and locks after about 15 minutes of inactivity (same idea as the web app).

Safari and mobile browsers: use the web app; there is no store extension.

11. Public tools

Under Tools: Generator — random passwords or memorable passphrases (IT/EN) with a cryptographic generator in the browser. Nothing is sent to the server. It is also embedded when you add a vault password.

Encrypt text (/tools/cipher) — seal or open text with a password you choose, always in the browser. It is not linked to the vault or the recovery key: forget that seal password and the sealed text is gone for good.

12. Profile and preferences

In Profile you can set an optional display name and name fields (stored inside vault ciphertext), page sizes, language, unlock landing, and auto-lock minutes.

Product/service email consent is an account setting on the server (opt-in, off by default). You can enable it at registration or in Profile. Encryptio never attaches vault contents to email.

13. Support and good practice

Under Support you will find this PDF manual, the FAQ, and Contact. What's new and How it works are under Product. For product ideas use Suggestions (after sign-in): never paste passwords or vault contents.

Keep the recovery key offline, and Legacy contact keys if you use Digital Legacy. Do not share your master password. After a local export, treat the file as sensitive material.

14. Server backups (security policy)

Encryptio runs automatic nightly backups of the service database: a full service copy, typically retained for about 30 days. Backups hold sealed vault data and account metadata only — never your master password or vault key in the clear.

From that global backup an operator can, when needed, also restore a single account deleted by mistake (within retention). This is not a self-service vault version history in Profile, and it does not replace a local JSON/CSV export on your computer.

Restore point: both disaster recovery and a single-account restore bring data back only as of the last successful nightly backup (normally the previous night). Later changes are not in that restore. You accept this explicitly at registration together with the Terms and Privacy Policy.

If you forget the master password without a recovery key, neither backups nor Encryptio can reopen the vault. Details in the Privacy policy and FAQ.