

NODRIVE

Backup, Recovery & Data Loss Policy

How to protect data and understand Beta limitations

Version 1.0 • 23 August 2026 • Beta

Contents

1. Core Principle
2. Password and Recovery Key
3. User Key and Moving to a New PC
4. Local Disks
5. Your Storage
6. Trash, Versions and Snapshots
7. Diagnostics and Support
8. Before Deleting a Disk or Account

1. Core Principle

Nodrive is not a backup replacement

During the Beta, do not use Nodrive as the only copy of important data. Keep at least one independent copy and periodically verify that it can be restored.

2. Password and Recovery Key

The password protects access to key material; a weak password can make an offline attack more practical if an attacker obtains the necessary encrypted material. The recovery key, where available, should be stored separately from the device and data it protects. Loss of the password and available recovery mechanisms may make data unrecoverable.

3. User Key and Moving to a New PC

In the current Beta the wrapped User Key remains on the local device and is not kept by the backend as a recovery copy. Before changing PC, formatting, uninstalling or deleting Nodrive local data, keep the recovery key and create/verify an Export backup where that feature is available. Merely signing into the Nodrive account on another computer should not be treated as a guarantee that keys can be recovered.

4. Local Disks

For local disks, availability depends on the storage selected by the user. HDD/SSD failure, loss or removal of a USB drive, filesystem damage, accidental deletion or loss of the device can make encrypted data unavailable. Keep a separate copy on a different medium or in a different location.

5. Your Storage

For Google Drive, WebDAV, NAS or other connected storage, continuity also depends on the user's provider or infrastructure. Account suspension, revoked or expired tokens, exhausted quota, API limits, synchronisation errors or object deletion can prevent access. Fiscalbox does not control these events.

For Google Drive, the Google account belongs to the user and the OAuth token is stored only locally. Revoking the token stops Nodrive access but does not automatically remove encrypted blocks already stored in Drive.

6. Trash, Versions and Snapshots

Trash, versions, snapshots or other recovery features, when present in the build and storage type in use, are additional recovery tools but are not a substitute for an independent backup. Check the app for the features actually available before relying on them.

7. Diagnostics and Support

Diagnostics sent to the Fiscalbox team are optional and intended to identify technical problems. They are not a backup service and are not used to store copies of user data. Support: info@nodrive.cloud.

8. Before Deleting a Disk or Account

1. Export the data you want to keep.
2. Verify the export by opening a sample of the files.
3. Keep recovery keys and backups in a separate place where relevant.
4. Check objects still stored with the provider selected by the user.
5. Remember that deleting the Nodrive account does not automatically delete data stored on a PC, NAS, Google Drive or another provider.