D

Data Loss: Causes, Recovery Steps, and Prevention

Data loss means information is deleted, corrupted, or unavailable. Learn immediate recovery steps and how tested, isolated backups limit the impact.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is data loss?
02 Common causes
03 What to do immediately
04 Recovery by situation
05 How to prevent data loss
06 Data-loss prevention vs. backups

Quick answer: Data loss occurs when information is deleted, corrupted, destroyed, or no longer accessible. Stop writing to the affected storage, preserve the original device or account, and identify whether the cause is deletion, hardware failure, ransomware, or an access problem. Recover from a verified backup or use qualified specialists rather than experimenting on the only copy.

01 What is data loss?

Data loss is the loss of availability or integrity of information. A file may be accidentally deleted, overwritten, encrypted by ransomware, corrupted during a failed update, or trapped in an account whose credentials or encryption keys are unavailable. The result can affect one document, an entire device, a cloud tenant, or a business-critical database.

Data loss is not the same as a data breach. A breach concerns unauthorized access or disclosure; data loss concerns deletion, damage, or inability to retrieve information. One incident can cause both—for example, ransomware operators may steal files before encrypting them.

02 Common causes

- Accidental deletion, overwrite, formatting, or incorrect synchronization.
- Storage device failure, power loss, overheating, or physical damage.
- Ransomware, destructive malware, malicious insiders, or compromised administrator accounts.
- Application bugs, failed migrations, database corruption, or bad automation.
- Cloud retention expiry, deleted SaaS accounts, misconfigured lifecycle rules, or provider outages.
- Lost passwords, multifactor access, recovery codes, encryption keys, or key-management services.
- Fire, flood, theft, and other events affecting both the primary system and nearby backups.

03 What to do immediately

1. **Stop changes:** pause synchronization, scheduled jobs, cleanup tools, and writes to the affected volume. Deleted blocks may be overwritten.
2. **Preserve the source:** do not reinstall the operating system, reformat the disk, or run unverified repair utilities on the only copy.

3. **Determine scope:** record the last known good time, systems, accounts, file paths, error messages, and people affected.
4. **Contain malicious activity:** if ransomware or account compromise is suspected, isolate affected systems and revoke attacker access while preserving evidence.
5. **Check recovery options:** review recycle bins, version history, snapshots, replicas, provider retention, and offline backups.
6. **Recover safely:** restore to a separate location when possible, scan it, validate key records, and only then return it to production.

A clicking drive, repeated disconnects, smoke, water damage, or firmware errors may indicate physical failure. Power it down and consult a reputable recovery laboratory. Repeated attempts can make recovery harder.

04 Recovery by situation

For a deleted local file, stop using the volume and check snapshots or backups before recovery software. For cloud storage or SaaS, contact the administrator or provider quickly because trash and version retention are time-limited. For a damaged database, preserve logs and a copy of the files, then restore and replay transactions in a separate environment. For ransomware, rebuild from trusted media and restore only after the intrusion path and persistence are addressed.

05 How to prevent data loss

Maintain multiple copies on different storage, including at least one isolated or offline copy that ordinary administrator credentials cannot delete. Versioning and immutable retention reduce the effect of malicious or accidental changes. Encryption protects confidentiality, but it does not replace backups; make sure encryption keys and recovery codes are backed up separately and securely.

Define a recovery point objective (RPO), the maximum acceptable data gap, and a recovery time objective (RTO), the maximum acceptable outage. These targets determine backup frequency, architecture, staffing, and cost. Monitor backup jobs, but also test full restoration regularly. A

successful backup log does not prove the data can be recovered.

06 Data-loss prevention vs. backups

Data-loss prevention (DLP) tools focus mainly on detecting and controlling sensitive data movement. Backups and resilience controls restore availability after deletion, corruption, or outage. Organizations often need both: DLP can reduce unauthorized disclosure, while isolated, tested backups reduce operational loss.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com