Backups: what must you back up, and would restores work?

This quarter, agree with each system's owner how much data it may lose and how long it may be down, and check that your backups cover every system, SaaS service and configuration, with one copy outside each provider's account. Then restore something every month, from single files to whole systems and SaaS apps, and treat any target you haven't met in a test as unmet.

Reviewed	Next review	Version
4 Nov 2026	**4 Dec 2026**	**1.0**

Written for

IT teams in small, mid-size and large organizations with on-premises servers, virtualization, Microsoft 365 or Google Workspace, other SaaS and cloud workloads

Latest version

sheets.einblick.dev/backups/

If you only do five things

1. **Let each system's owner set its targets.**
   Ask how much data it may lose (RPO) and how long it may be down (RTO). The business decides; IT makes it happen.
2. **Back up what the provider won't restore.**
   Your data and configuration stay yours to protect in SaaS too[3]. Keep an independent copy in another service[4].
3. **Keep a copy outside the platform it protects.**
   In 2024 a Google error deleted a customer's VMware Engine private cloud without notice. Backups kept in Cloud Storage, outside the deleted private cloud, helped restore it[5].
4. **Check coverage weekly, not just job status.**
   Alert on any system without a recent restore point. New servers, sites and SaaS apps are the usual gaps.
5. **Restore something every month.**
   Rotate a file, a mailbox, a server and a SaaS app, and have the owner check each. The ransomware sheet covers the full test.

Set scope and targets with the business

1. **What do you run?**
   Take the asset inventory and add SaaS from invoices and single sign-on. Include network devices: they store configuration too[2].
2. **How much loss and downtime can each system take?**
   Agree RPO and RTO with the owner, within the business continuity sheet's process limits, plus the legal and deletion needs the BSI lists[2]. Base backup frequency on criticality and change rate[1].
3. **How far back must you go?**
   Set retention from the slowest loss anyone would notice.
4. **Can the method meet the target?**
   Check that restore bandwidth fits the RTO, and that online backup contracts state location, SLA and encryption[2].
5. **Can you reach the plan in a crisis?**
   Write one page per system: what, how, how long, restore order, owner. Keep it where it survives the backup system[2].

What people forget to back up

- **SaaS beyond mail and files.** CRM, ticketing, wikis, HR, finance. Atlassian's backup add-on keeps copies only 30 days[6].
- **Repositories and CI.** GitHub's migration archives skip LFS objects, discussions and packages, and GitHub has no supported way to restore them[7]. Self-managed GitLab backups omit `gitlab-secrets.json`, which holds the key to 2FA data and CI/CD variables[8].
- **Tenant configuration.** Microsoft Graph can snapshot Microsoft 365 tenant settings, but deletes each snapshot after 7 days[9]. Export them.
- **BitLocker keys.** Deleting an Entra device deletes them for good[10].
- **Network configs and the admin vault.** Export DNS zones and device configs after each change, and keep an encrypted vault export offline.

What SaaS providers restore, and for how long

- **Exchange Online.** Deleted items are recoverable 14 days by default, 30 at most[11]. A deleted mailbox without a hold is gone after 30 days[12].
- **SharePoint and OneDrive.** The recycle bin keeps items 93 days. After that, Microsoft support can roll back only a whole site or subsite, within 14 more days[13]. A deleted user's OneDrive is kept 30 days by default, then 93 days in the recycle bin[14].
- **Microsoft 365 Backup.** It covers SharePoint, OneDrive and user and shared mailboxes, not group or room mailboxes[16]. Its copies stay inside Microsoft 365[15].
- **Google Workspace.** Admins can restore Drive files for 25 days after the trash is emptied[17] and deleted users for 20 days[18]. Google says Vault isn't designed as a backup tool[19].

How far back to keep

- **Keep dailies 35 days and monthlies 12 months.** That spans a month-end close, and the 35 days match AWS Backup's default audit control[20].
- **Know what versioning keeps.** With an expiry limit, SharePoint files nobody edits can lose every version[21]. Raise Exchange's deleted item retention to 30 days[11].
- **Archive records; don't keep backups for years.** The BSI treats long-term retention as archiving[2]. Meet tax and legal retention in a records system.
- **Let personal data age out.** A fixed retention period does that. The retention and deletion sheet covers erasure requests and restores.

Prove coverage and restores

- **Find what nothing protects.** AWS Backup Audit Manager flags resources outside any backup plan or without a recent recovery point[20].
- **Alert on silence.** A job that never starts raises no failure, and full storage can stop backups or overwrite old ones unnoticed[2].
- **Test small and large restores.** ENISA's NIS2 guidance suggests testing full system and single file restores, validated by business users[22]. In tests, restore SaaS to a new location, not over production.
- **Automate in the cloud.** AWS Backup can restore a random recovery point on a schedule, time it and delete it[23].

What changed in 2026

- **Microsoft 365 Backup restores single files and keeps longer.** Granular file restore has been generally available since September 2026, for the last 14 days. Recovery windows have been configurable since September, and since 31 October reach 10 years for SharePoint and OneDrive[16].
- **Microsoft 365 Backup catches new items.** Full Workload Backup, in preview since September 2026, adds eligible sites, OneDrives and mailboxes that no policy covers[16].
- **AWS air-gapped vaults take more workloads.** Since March 2026 they accept Amazon EKS backups, which can be shared for recovery across accounts and AWS Organizations[25].

What you can skip

- **Image backups of laptops.** If files sync to OneDrive or Google Drive and Intune or Autopilot rebuilds devices, reinstall instead.
- **Whole-VM backups of servers built from code.** Back up the data, the code and the secrets.
- **One schedule for everything.** NIST bases frequency on criticality and change rate[1]. Most file shares are fine with daily backups.
- **Decade-long backup retention.** It multiplies cost and erasure work. Archive what the law requires.

Mistakes that cost the most

- **Deleting a leaver's account first.** The mailbox is gone 30 days later[12], a Google account after 20 days[18].
- **Counting RAID or replication as a backup.** A mirror changes with the original, so overwrites and malware hit both[2].
- **Keeping cloud backups in one region.** Azure's Cross Region Restore needs a geo-redundant vault, set before the first backup[24].
- **Trusting a green dashboard.** Jobs can succeed while skipping new systems. Only a restore proves a backup.

What this looks like at your size

Small team, no security staff

- Raise Exchange deleted item retention to 30 days, and move a leaver's OneDrive files before deleting the account.
- Keep a printed page per system: owner, what's backed up, where, how to restore.
- Restore one file and one mailbox item every month and write down how long it took.

Growing, with IT or security staff

- Spend an hour with each system owner on RPO, RTO and retention, and get their sign-off.
- Send a weekly report of assets without a recent restore point to a named person.
- Back up repositories, CI settings and tenant configuration, not just data.

Enterprise or regulated

- Cloud, data center, managed service and other digital providers under NIS2 need backup plans covering configuration and cloud data, distant copies and retention, plus integrity checks[22].
- Report measured restore times against RPO and RTO per system each quarter.
- Copy critical SaaS and cloud data to a second provider and restore from it yearly.

Version history

4 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which corrected the OneDrive leaver advice and narrowed 8 statements to what the sources say.

Sources

1. SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. NIST, May 2010. nvlpubs.nist.gov
2. IT-Grundschutz, CON.3 Datensicherungskonzept. BSI, Edition 2023. bsi.bund.de
3. Shared responsibility in the cloud. Microsoft Learn, 24 Aug 2026. learn.microsoft.com
4. Back up your organisation's critical data. NCSC (UK), 11 Jan 2024. ncsc.gov.uk
5. Details of Google Cloud GCVE incident. Google Cloud, 24 May 2024. cloud.google.com
6. Overview of Atlassian Backup and Restore. Atlassian Support, checked 4 Nov 2026. support.atlassian.com
7. Backing up a repository. GitHub Docs, checked 4 Nov 2026. docs.github.com
8. Back up GitLab. GitLab Docs, checked 4 Nov 2026. docs.gitlab.com
9. Use the Tenant Configuration Management APIs in Microsoft Graph. Microsoft Learn, 19 Jan 2026. learn.microsoft.com
10. Manage stale devices in Microsoft Entra ID. Microsoft Learn, 27 Jun 2025. learn.microsoft.com
11. Recoverable Items folder in Exchange Online. Microsoft Learn, 25 Sep 2026. learn.microsoft.com
12. Delete or restore user mailboxes in Exchange Online. Microsoft Learn, updated 3 Aug 2026. learn.microsoft.com
13. Microsoft 365 SharePoint data deletion. Microsoft Learn, 28 Aug 2026. learn.microsoft.com
14. OneDrive retention and deletion. Microsoft Learn, 2 Jun 2026. learn.microsoft.com
15. Overview of Microsoft 365 Backup. Microsoft Learn, 4 Nov 2026. learn.microsoft.com
16. What's new in Microsoft 365 Backup. Microsoft Learn, 4 Nov 2026. learn.microsoft.com
17. Recover deleted files and folders for Drive users. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
18. Restore a recently deleted user. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
19. Google Vault FAQ. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
20. Controls and remediation (AWS Backup Audit Manager). AWS Docs, checked 4 Nov 2026. docs.aws.amazon.com
21. Plan version storage for document libraries. Microsoft Learn, 29 May 2025. learn.microsoft.com
22. NIS2 technical implementation guidance, v1.0. ENISA, 26 Jun 2025. enisa.europa.eu
23. AWS Backup restore testing. AWS Docs, checked 4 Nov 2026. docs.aws.amazon.com
24. Create and configure Recovery Services vaults. Microsoft Learn, 10 Dec 2025. learn.microsoft.com
25. AWS Backup adds logically air-gapped vault support for Amazon EKS. AWS, 12 Mar 2026. aws.amazon.com