ELEVATE
SOLUTIONS

GUIDE · BUSINESS & INDUSTRY

Backup & Disaster Recovery Guide

The 3-2-1-1-0 rule

The 3-2-1-1-0 backup rule explained — why every component matters, plus RTO and RPO in plain English, and the architecture a recovery-grade backup stack is built on.

01 — THE RULE

3-2-1-1-0, digit by digit

A backup is not a product you bought. It is a recovery you can prove. The 3-2-1-1-0 rule is the simplest standard that survives contact with a real incident — including the one where the attacker goes after your backups first.

Ransomware appeared in 44% of breaches, up 37% year over year. Verizon DBIR 2025 Modern ransomware operators do not encrypt on arrival. They spend time inside the network first, and one of their first objectives is to find and destroy anything you could restore from. Every digit in 3-2-1-1-0 exists because some firm, somewhere, lost data while believing it was protected.

3 — Three copies of your data

The production copy plus at least two backups. Any single copy can be lost to hardware failure, human error, corruption, or attack. Two backups means one failure during recovery does not end the recovery. If your "second copy" is a replica that mirrors production in real time, it mirrors the damage in real time too — it counts toward availability, not toward three copies.

2 — Two different media or platforms

The two backup copies should not share a failure mode. Two folders on the same NAS share every failure mode: firmware bug, controller fault, stolen device, encrypted volume. Different media means different platforms with different administration — for example, a local backup appliance plus cloud object storage, or disk plus tape. The question to ask: what single event could take both copies at once? If you can name one, they are not two media.

1 — One copy offsite

Fire, flood, theft, and a building you cannot enter for two weeks are all recoverable events — if a copy exists somewhere else. "Offsite" means a different failure domain: a different building and a different network, not the far end of the same office or a drive in a desk at home. For most firms today the offsite copy is cloud storage in a provider's data center, which also solves the problem of someone remembering to carry media.

1 — One copy offline or immutable

This is the digit ransomware added to the rule, and it is now the one that decides outcomes. An offline or immutable copy cannot be altered or deleted from the production network — not by malware, and not by an administrator account, because the attacker will have an administrator account. Attackers who reach the backup console delete or encrypt the backups before detonating ransomware, precisely so the only path back is the ransom. Section 03 covers how to build this copy properly.

0 — Zero errors, meaning verified restores

A backup that has never been restored is a hypothesis. Zero errors means backup jobs complete without errors, verification runs automatically, and a human actually performs restores on a schedule and records the results. Section 04 is the testing checklist.

WHY THE SECOND "1" IS NON-NEGOTIABLE

Backups are the first target, not the last line. If every copy of your data can be reached and deleted with credentials that exist inside your network, you do not have a backup strategy — you have a single point of failure with extra steps.

Three things that are not backups

THE BELIEF	WHY IT FAILS WHEN YOU NEED IT
"It's in OneDrive / Dropbox" Sync ≠ backup	Sync tools replicate changes — including encryption and deletion — to every device and to the cloud copy within minutes. File versioning can rescue a single document; it is not built for restoring a hundred thousand files to a known-good point in time, version history has limited retention windows, and an attacker holding the account or the admin role can empty the recycle bin and purge versions.
"The server has RAID" RAID ≠ backup	RAID is availability, not recoverability. It keeps the system running through a disk failure — and it faithfully preserves every deletion, corruption, and ransomware encryption across all disks instantly. A controller fault, a second disk dying mid-rebuild, or a fire takes the whole array. RAID answers "will it stay up?", never "can I go back?"
"We have retention policies" Retention ≠ backup	Retention and litigation hold keep data for compliance and discovery — inside the same platform, the same tenant, and the same administrative blast radius as the data they retain. A compromised or misconfigured admin role threatens both at once. Section 02 covers the Microsoft 365 / SaaS decision this implies.

02 — TARGETS

RTO and RPO in plain English

Two numbers turn "we have backups" into a plan: how much data you can afford to lose, and how long you can afford to be down.

RPO — Recovery Point Objective. The maximum age of the data you restore; everything created after the last good backup is gone. Measured backward from the incident. An RPO of 4 hours means you accept losing up to 4 hours of work.

RTO — Recovery Time Objective. How long until the system is usable again. Measured forward from the moment you decide to restore. An RTO of 8 hours means the business can tolerate one working day without that system.

Memory aid: RPO is data lost, RTO is time lost.

Set targets per system, not per company

One blanket target either overspends on systems that do not matter or underprotects the ones that do. For each system, ask what an hour of lost data and an hour of downtime actually cost — in billable work that cannot be reconstructed, missed filing deadlines, patient-care disruption, payroll, and regulatory or client exposure. The answers cluster into tiers, and the tiers set the targets.

As planning ranges we use for regulated professional firms — guidance, not a standard — Tier 1 systems (practice management, EHR, billing, the document store) usually land at an RPO of 1 hour or less and an RTO of 2–8 hours. Tier 2 (file shares, line-of-business apps) at an RPO of 4–24 hours and an RTO of 1–2 days. Tier 3 (archives, reference data) at an RPO of 24 hours or more and an RTO measured in days. Your numbers may differ; the point is that they are decided by business impact, written down, and owned by someone.

The cost curve

Tighter targets cost more, and the curve is steep at the end. Moving an RPO from 24 hours to 4 hours is usually a scheduling change. Moving it from 1 hour to near-zero means continuous replication. Moving an RTO from days to hours means standby infrastructure that exists only to wait. None of that is wasted on a system the business stops without — all of it is wasted on a system nobody would miss for a week. Match targets to impact, not to a vendor's default policy or the tightest number that sounds safe.

Worksheet: targets by system

The first row is a worked example. Fill in the rest with your own systems, set targets, and have the owner — the person accountable for that system's recovery — confirm each row.

SYSTEM	TARGET RPO	TARGET RTO	OWNER
Practice management (example)	*1 hr*	*4 hrs*	*Ops director*

MICROSOFT 365 AND SAAS DATA: MAKE THE DECISION EXPLICITLY

SaaS platforms operate on a shared-responsibility model: the provider keeps the service running; protecting your data in it remains your decision. Built-in retention, recycle bins, and litigation hold serve compliance and discovery — they were not designed as a backup service, and they live inside the same tenant and admin plane they would need to protect. Whether to back up Microsoft 365 (Exchange, SharePoint, OneDrive, Teams) and other SaaS data to separate, independently controlled storage is a decision your firm should make deliberately, document, and revisit — not inherit from defaults.

03 — RESILIENCE

Immutability and air-gap

The copy that saves you is the one the attacker could not touch. Building it takes more than a checkbox labeled "immutable".

What immutable actually means

An immutable backup is written once and cannot be modified or deleted until a retention timer expires — enforced by the storage platform, not by policy. The common mechanisms: **object lock** on cloud object storage (write-once, read-many for a set period) and **retention lock** on backup appliances. The detail that matters is the enforcement mode: in compliance-style modes, nobody can shorten or remove the lock during the window — not your admin, not the vendor's support desk under social-engineering pressure. Governance-style modes that privileged accounts can override are a speed bump, not a wall.

Size the immutability window against detection time, not convenience. Across all organizations the mean time to identify and contain a breach was 241 days. IBM Cost of a Data Breach Report 2025 You will likely detect ransomware much faster — it announces itself — but quiet compromise can precede it by weeks. An immutable window of 7 days, with no deeper restore points behind it, can leave every reachable copy inside the compromise period. Pair a 14–30 day immutable window with longer-term restore points (weekly, monthly) so a clean copy exists behind any plausible dwell time.

Air-gap options

APPROACH	WHAT IT LOOKS LIKE	WATCH OUT FOR
Physical offline	Tape, or rotated disks disconnected and stored in a safe or offsite. Nothing on a wire can touch a cartridge on a shelf.	Depends on human discipline; restore is slow; media ages and must be test-read.
Logical air-gap	A cloud copy in a separate account or tenant with its own credentials, no trust relationship with your domain, ideally pull-based so production holds no write keys to it.	Only as isolated as its identity. Shared admin email, reused passwords, or SSO from the corporate tenant quietly close the gap.

Separate the backup identity plane

Attackers delete backups first, and they do it with stolen admin credentials. So the backup console must not trust the credentials they steal. In practice: backup consoles and backup storage accounts use dedicated accounts that exist nowhere else — not domain-joined, not in corporate SSO, not your day-to-day admin account. MFA on every one of them. Alerts fire when retention settings change or large deletions are requested, and where the platform offers a deletion delay or two-person approval for destructive actions, turn it on.

Encrypt the backups themselves

Backups are a complete, portable copy of your most sensitive data — client files, PHI, financial records — often sitting in more places than production. Encrypt them in transit and at rest, and treat key custody as seriously as the backups: document where the encryption keys and passphrases live, who can reach them, and how they are recovered if the primary key holder is unavailable. A backup whose key is lost is not a backup. A backup whose key is taped to the appliance is not encrypted.

What a well-built stack includes, and why

Whoever operates your backups — internal IT or an outside provider — a stack that holds up under an incident, an audit, and an insurance claim has these properties. Use this list to evaluate what you have, not to shop for a logo.

- [ ] **Image-based backup of servers and critical endpoints** 1
  Full-system images, not files alone — so a dead server can be rebuilt as a working machine within the RTO, not reconstructed application by application.
- [ ] **An offsite copy on immutable storage** 2
  Object lock or retention lock, in a compliance-style mode, with the window sized as described above.
- [ ] **An explicit, documented SaaS backup decision** 3
  Microsoft 365 and other SaaS data either backed up to independent storage or consciously accepted as a risk — in writing, with a named decision owner.
- [ ] **A backup identity plane separated from production** 4
  Dedicated credentials, MFA, no domain trust, alerts on retention changes and deletions.
- [ ] **Automated verification plus a human who acts on failures** 5
  Boot or integrity checks on every job, and failure alerts routed to a person whose job is to fix them that day — not to a mailbox nobody reads.
- [ ] **A written recovery runbook** 6
  Restore order, system dependencies (identity and DNS before applications), key custody, and who declares a disaster — current and stored where a ransomware event cannot encrypt it.
- [ ] **Restore testing on a calendar, with evidence** 7
  The schedule and proof in Section 04. Speed matters: breaches contained in under 200 days averaged $3.61M versus $5.49M for those that ran longer. IBM Cost of a Data Breach Report 2025

04 — VERIFICATION

Recovery testing checklist

The "0" in 3-2-1-1-0 is earned quarterly, not assumed. Run this checklist on a schedule, record the results, and keep the records.

- [ ] **Quarterly file-level restore** 1
  Restore a sample of files and folders from each major system to a known-good point in time. Confirm contents, permissions, and timestamps — not just that the job reported success.
- [ ] **Annual full-system restore** 2
  Rebuild at least one production server from image backup as a complete, bootable machine. This is the test that finds missing drivers, broken boot configs, and undocumented dependencies.
- [ ] **Documented restore times measured against RTO** 3
  Time every test from "restore initiated" to "system usable" and compare against the worksheet in Section 02. A 12-hour actual against a 4-hour target is a finding, not a footnote.
- [ ] **Test a restore from the immutable copy** 4
  At least annually, restore from the offline or immutable copy specifically — the copy you would depend on if ransomware destroyed everything reachable. Confirm the lock held and the data is intact.
- [ ] **Restore to an isolated network** 5
  Bring restored systems up on a segment with no path to production. This mirrors real ransomware recovery — you cannot restore into a network that is still hostile — and prevents test restores from colliding with live systems.
- [ ] **Application-level validation, not just files** 6
  After restoring, log in to the application. Open a client matter or patient record, run a report, post a test transaction. Databases and line-of-business apps can restore "successfully" as files and still be unusable.
- [ ] **Backup-console MFA and credential separation verified** 7
  Confirm the backup console and backup storage still require MFA, still use dedicated non-domain credentials, and that no production admin account has quietly acquired access since the last check.
- [ ] **Alert-on-failure tested end to end** 8
  Deliberately trigger or simulate a failed job and confirm an alert reaches a person who acts. An alerting path is only proven by a test that fires it.
- [ ] **Recovery runbook reviewed and current** 9
  Verify restore order, contacts, key custody, and system inventory against reality. Update for anything added, retired, or migrated since the last review, and confirm an off-network copy exists.
- [ ] **Evidence retained for your insurer and auditor** 10
  Keep dated test logs, screenshots, timings, and sign-offs. Cyber insurance applications and renewals increasingly ask whether backups are tested; regulators and clients ask too. Records you kept are the answer.

Record of last test

Date of last file-level restore test _____

Date of last full-system restore test _____

Measured restore time vs. RTO target _____

Tested by / sign-off _____

ELEVATE SOLUTIONS

Elevate Solutions provides managed IT and cybersecurity for businesses that answer to regulators, clients, and courts.

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io