CLOUDSWITCHED

FREE RESOURCE — BACKUP STRATEGY PLANNING GUIDE

Backup Strategy Planning Guide

A practical guide to designing a backup strategy that survives ransomware, hardware failure and a panicked Tuesday morning. Apply the 3-2-1-1-0 rule, classify every system honestly, pick retention that matches your obligations, and lock in a test schedule so the day you need a restore is not the day you discover it never worked.

3-2-1-1-0
MODERN BACKUP RULE

Immutable
RANSOMWARE-PROOF COPY

Monthly
RESTORE-TEST CADENCE

Fillable
TICK & TYPE IN ANY VIEWER

3-2-1-1-0 | IMMUTABLE | M365 BACKUP | AUDIT-READY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this guide

This guide covers the six decisions every backup strategy has to answer: **which rule are you following** (3-2-1, or the stricter 3-2-1-1-0), **what data needs protecting** and at what priority, **how is each system configured**, **how long do you keep it**, **how do you prove the backups actually work**, and **who owns it all**. Read it once, fill in the worksheets, then review them every quarter — the value comes from the document being current, not pristine.

> **A BACKUP YOU HAVE NEVER RESTORED IS NOT A BACKUP**
>
> The single most common failure mode in a real ransomware or hardware-loss event is a backup that looked healthy in the console but cannot actually be restored. Section 05 builds a real test calendar — commit to a monthly file restore, a quarterly full-system restore and an annual DR-grade exercise. Record every result; that evidence is what Cyber Essentials, ISO 27001 and your cyber insurer will ask for.

The six planning sections

- **01 The 3-2-1 Backup Strategy** — the rule, the modern 3-2-1-1-0 extension, and your current setup.
- **02 System Criticality & What to Back Up** — classify every data source, method, frequency, retention and priority.
- **03 Backup Configuration Best Practices** — encryption, immutability, monitoring, versioning, bandwidth.
- **04 Retention & Encryption Strategy** — tiered retention that matches your legal and business obligations.
- **05 Testing & Validation** — the test types, cadence and a real calendar to record measured restores.
- **06 Ownership & Sign-off** — who runs which backup, who reviews the strategy, and quarterly sign-off.

Roles to agree before you commit to a backup strategy

- **Backup Owner** — single accountable person for the overall strategy; signs off retention and recovery targets.
- **Technical Lead** — configures the backup product, monitors daily health, drives restore tests on schedule.
- **Business Owner (per system)** — sets the recovery priority and retention for each system they own.
- **Reviewer** — quarterly review of restore-test evidence; escalates failed or skipped tests.

01

The 3-2-1 Backup Strategy

The 3-2-1 rule is simple but unreasonably effective: **3 copies** of your data, on **2 different media types**, with **1 copy offsite**. The modern **3-2-1-1-0** extension adds the two things ransomware actually demands: **1 immutable copy**, and **0 errors** proven by regular restore testing.

Reference: the 3-2-1-1-0 rule decoded

DIGIT	WHAT IT MEANS	WHAT IT PROTECTS AGAINST
3 copies	Production data + 2 separate backups	Hardware failure, accidental delete
2 media types	e.g. local disk + cloud object storage	Single-medium failure (NAS dies, account locked)
1 offsite	Cloud or geographically remote location	Fire, flood, theft of the building
1 immutable	Object Lock, WORM, air-gapped vault	Ransomware targeting backup repositories
0 errors	Verified by scheduled restore tests	Backups that will not actually restore

Your current 3-2-1-1-0 setup

Write down what is in place today — honestly. The gap between this worksheet and the rule above is your real backup risk register.

3-2-1-1-0 ELEMENT	WHAT YOU HAVE TODAY	STATUS
3 copies (production + 2 backups)		
2 media types		
1 offsite copy		
1 immutable copy		
0 errors (proven by tests)		

MICROSOFT 365 DOES NOT BACK UP YOUR DATA

Microsoft 365 retention is short-term, user-driven recovery (recycle bin, version history) — not backup. It does not protect against ransomware, malicious deletion or a tenant compromise. A third-party M365 backup product (Veeam, Datto, AvePoint, Acronis) is mandatory for Exchange Online, OneDrive, SharePoint and Teams — treat M365 as a row in Section 02.

02

System Criticality & What to Back Up

Identify every data source that needs protection, then assign a backup method, frequency, retention and priority to each. Anything not on this list is implicitly "we can lose it" — so be exhaustive: include SaaS apps, network configs and endpoint data, not just servers.

Reference: typical backup posture by data source

DATA SOURCE	RECOMMENDED METHOD	FREQUENCY	PRIORITY
Microsoft 365 (mail, OneDrive, SharePoint, Teams)	Third-party M365 backup	3× daily	Critical
On-premise file / image server	Cloud backup agent + image backup	Daily	Critical
SQL / database server	Native DB backup + cloud copy	Every 4 hours	Critical
Endpoint (laptop) data	OneDrive redirect / endpoint backup	Continuous	Medium
SaaS & network configs	Vendor export / 3rd-party SaaS backup	Daily / per change	High

Your system criticality register

One row per system. The Business owner signs off priority and retention; the Tech owner runs the backup.

DATA SOURCE / SYSTEM	BACKUP METHOD	FREQUENCY	RETENTION	PRIORITY	OWNER

DO NOT FORGET YOUR SAAS DATA

Any SaaS app holding business data — CRM, accounting, helpdesk — belongs on this list. If the vendor has no usable export, a third-party SaaS backup is the only safety net if the account is deleted, breached or the vendor disappears.

03

Backup Configuration Best Practices

The configuration choices below are what separates a backup that actually restores from one that quietly fails the day you need it. Tick each item as you verify it for your environment; an unticked box is an open risk on the strategy.

Encryption & integrity

- ☐ **Encryption at rest** — AES-256 enabled on every backup repository (cloud and on-prem).
- ☐ **Encryption in transit** — TLS 1.2 or higher between every backup agent and its repository.
- ☐ **Key custody** — encryption keys stored separately from the backup data, with documented escrow.
- ☐ **Integrity checks** — the backup product runs scheduled checksum / health verification on stored backups.

Ransomware resilience

- ☐ **Immutable storage** — at least one copy is write-once (Object Lock, hardened repository, or vault).
- ☐ **Separate identity** — backup admin accounts live in a different identity scope from production admins, with MFA enforced.
- ☐ **No live backup share** — production servers cannot reach backup storage with read-write SMB / NFS credentials.
- ☐ **Air-gap / vault** — for Tier 1 data, a copy is held in an isolated location that is unreachable from the production network.

Monitoring, scheduling & versioning

- ☐ **Failure alerting** — every failed or skipped backup raises an alert investigated within 4 hours.
- ☐ **Daily dashboard review** — backup posture (jobs run, jobs failed, capacity) reviewed every working day.
- ☐ **Window scheduling** — large full backups run outside business hours; incremental / differential backups carry the daily load.
- ☐ **Versioning** — enough versions retained to recover from slow data corruption that may not be noticed for weeks.
- ☐ **Documentation** — restore runbook lives outside the systems being backed up (printed, or in a separate tenant).

04

Retention & Encryption Strategy

Retention is two questions at once: **how far back** can you recover, and **for how long** must you be able to produce the data. The first is a business decision driven by recovery scenarios; the second is set by law, regulation and your insurer. A tiered retention plan (daily □ weekly □ monthly □ annual) lets both live together without paying to keep every nightly backup forever.

Reference: a sensible default retention ladder

TIER	KEPT	WHY THIS LENGTH
Daily backups	30 days	Day-to-day recovery from accidental delete, file corruption, ransomware notice window
Weekly backups	12 weeks	Recover from gradual corruption noticed weeks later; quarterly trend recovery
Monthly backups	12 months	Year-on-year comparisons; recover data set the day before a major change
Annual / archive	7 years (or per law)	HMRC, ICO, sector regulators; cyber-insurance proof-of-record

Your retention worksheet

One row per regulated or business-critical data class. Pin retention to the obligation (legal or business) that drives it — that is what auditors will ask for.

DATA CLASS	RETENTION	OBLIGATION SOURCE	ENCRYPTION	IMMUTABLE?	OWNE

RETENTION IS NOT THE SAME AS BACKUP FREQUENCY

A backup taken hourly with 24 hours of retention will let you recover the last day — not the last month. Retention is what you keep on the shelf; frequency is how often you write a new copy onto it. Pick both deliberately. Cyber insurance underwriters specifically ask about retention, immutability and restore-test evidence — not just whether backups exist.

05

Testing & Validation

A backup that has not been restored is not a backup — it is a hope. The single biggest predictor of recovering successfully is how often you have actually run a restore. Pick a cadence per test type and stick to it; the auditors and your cyber insurer will both ask for the dated evidence.

Reference: minimum recommended cadence

TEST TYPE	CADENCE	WHAT IT PROVES
Individual file restore	Monthly	Selected files restore with correct content and permissions
Full system / VM restore	Quarterly	An entire server or VM can be brought back to a working state
Application-level restore	Quarterly	Database / LOB app restores and functions correctly after recovery
Bare-metal recovery	Bi-annually	A server can be rebuilt onto new hardware from backup alone
Disaster-scenario exercise	Annually	End-to-end recovery within the RTO target, including comms

Restore-test calendar & results

One row per test executed. Capture the **measured** outcome — the time it actually took, not the time you hoped it would take.

DATE	TEST TYPE	SCOPE & SCENARIO	TIME TAKEN	PASS / FAIL	OWNE

DOCUMENT EVERY TEST — NOT JUST THE FAILURES

Record the date, scope, result, time taken and any issues for every restore. That evidence is what Cyber Essentials, ISO 27001 and your cyber insurer will want to see. A clean pass log is also the cheapest way to prove due diligence after an incident.

06

Ownership & Sign-off

A backup strategy without a named owner is a backup strategy that quietly rots. This page assigns accountability for every backup product in use and sets a quarterly review rhythm so the strategy stays current as systems are added, retired or moved between tiers.

Backup product ownership register

BACKUP PRODUCT / SERVICE	PROTECTS	TECHNICAL OWNER	BUSINESS OWNER	NEXT REVIEW

Review cadence

- **Daily** — Technical Lead reviews backup dashboard, investigates every failed job within 4 hours.
- **Monthly** — one file restore test logged in Section 05.
- **Quarterly** — one full-system restore test, plus a review of this entire document with the Backup Owner.
- **Annually** — bare-metal / disaster-scenario exercise; renew retention and immutability decisions against current regulation.

PREPARED BY	DATE	APPROVED BY

Need a backup strategy built & run for you?

Cloudswitched designs, deploys and runs immutable 3-2-1-1-0 backup for UK SMEs — covering Microsoft 365, on-premise servers and SaaS data, with scheduled restore tests and audit-ready evidence on a fixed-fee retainer.

info@cloudswitched.com

cloudswitched.com/solutions/cloud-backup

CLOUDSWITCHED

CLOUD BACKUP & DATA PROTECTION

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom