Backup Strategy Planning Guide

3-2-1 backup strategy, frequency, retention, encryption, and testing. Build a comprehensive data protection strategy that safeguards your business against data loss.

3-2-1	Daily	Test	Free
BACKUP STRATEGY RULE	MINIMUM BACKUP FREQUENCY	MONTHLY RESTORE VERIFICATION	STRATEGY GUIDE

1 The 3-2-1 Backup Strategy

The gold standard for data protection that every organisation should follow.

The 3-2-1 rule is simple but powerful: maintain **3 copies** of your data, on **2 different media types**, with **1 copy offsite**. This protects against hardware failure, ransomware, theft, fire, and human error.

The 3-2-1 Rule

- ✓ 3 copies: original + 2 backups
- ✓ 2 media types: e.g., disk + cloud
- ✓ 1 offsite: cloud or remote location
- ✓ Protects against single point of failure

Modern Extension: 3-2-1-1-0

- ✗ 1 copy immutable (cannot be modified)
- ✗ 0 errors (verified with regular testing)
- ✗ Protects against ransomware deletion
- ✗ Ensures backup integrity

Microsoft Does Not Back Up Your Data

Microsoft 365 retention policies are designed for short-term recovery (recycle bin), not backup. They do not protect against ransomware, malicious deletion, or extended retention requirements. A third-party backup solution (Veeam, Datto, Acronis) is essential for M365 data.

2 What to Back Up

Identify all data sources that require backup protection.

DATA SOURCE	BACKUP METHOD	FREQUENCY	RETENTION	
Microsoft 365 (email, OneDrive, SharePoint, Teams)	Third-party M365 backup	3x daily	7 years	Critical
On-premise file server	Cloud backup agent	Daily (incremental)	90 days daily, 12 months monthly	Critical
On-premise server (system state)	Image-based backup	Daily	30 days	Critical
SQL/database server	Native DB backup + cloud copy	Every 4 hours	30 days	Critical
Line-of-business application data	Application-specific + file backup	Daily	Per compliance requirement	High
Endpoint (laptop) data	OneDrive redirect / endpoint backup	Continuous sync	30 days	Medium
Network device configurations	TFTP / cloud management export	After every change	90 days	High

Do Not Forget SaaS Data

Any SaaS application containing business data (CRM, accounting, project management) should be backed up. Check if the vendor provides data export/backup tools. If not, use a third-party SaaS backup solution.

3 Backup Configuration Best Practices

Configure backups for reliability, security, and recoverability.

- **Encryption:** All backups must be encrypted at rest (AES-256) and in transit (TLS 1.2+). Store encryption keys separately from the backup data.
- **Immutability:** Enable immutable backup storage where available. This prevents ransomware from deleting or encrypting your backup data.
- **Monitoring:** Configure alerts for backup failures. Every missed backup must be investigated within 4 hours.
- **Retention:** Align retention with legal requirements (7 years for financial data) and business needs. Use a tiered approach: daily backups retained 30 days, weekly 12 weeks, monthly 12 months, annual 7 years.
- **Bandwidth management:** Schedule large backups outside business hours. Use incremental/differential backups to minimise data transfer.
- **Versioning:** Maintain multiple backup versions to recover from gradual data corruption that may not be immediately noticed.

4 Testing & Validation

A backup that has not been tested is not a backup. Establish a regular testing schedule.

TEST TYPE	FREQUENCY	WHAT TO VERIFY	WHO PERFORMS
Individual file restore	Monthly	Selected files restore correctly with correct content	IT team
Full system restore	Quarterly	Complete server/VM can be restored to working state	IT team + vendor
Bare-metal recovery	Bi-annually	Server can be rebuilt from backup on new hardware	IT team + vendor
Application-level restore	Quarterly	Database/application restore and function correctly	IT team + app owner
Disaster recovery scenario	Annually	Full business recovery from backup within RTO target	IT team + management

Document Every Test

Record the date, scope, result, time taken, and any issues for every restore test. This evidence is required for Cyber Essentials, ISO 27001, and demonstrates due diligence to auditors and insurers.

Notes

Need a Backup Strategy Designed?

We design, implement, and manage comprehensive backup strategies that protect UK businesses from data loss.

info@cloudswitched.com

New London House, 6 London St, London EC3R 7LP

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.

cloudswitched.com