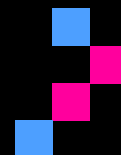


Data Backup & Recovery Planning Template



Initial
TECH

Initial Technology

Data Backup & Recovery Planning Template

Company Name
Prepared by
Approved by
Version

Overview

Use this simple, practical template to define how you back up critical data and how you will restore it. It is designed for small and mid-sized organisations and aligns with widely adopted best practices such as the 3-2-1 backup rule, ACSC Essential Eight (Regular Backups), ISO/IEC 27031, and NIST guidance. Keep it concise—aim for 6–12 pages. Review after any major change or at least quarterly.

1. Scope & Objectives

1.1 Scope	1.2 Objectives	1.3 Assumptions
Describe the business processes, systems, and locations covered by this plan (e.g., Microsoft 365, on-prem servers, cloud apps, endpoints).	Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each system, and the maximum tolerable downtime and data loss.	List any assumptions (e.g., internet connectivity available, vendor SLAs in place).

2. Roles & Responsibilities

Item	Notes
Plan Owner:	Maintains this plan and coordinates updates and tests.
Backup Admin:	Configures backup jobs, monitors success/failures, ensures immutability/offsite copies.
Restore Lead:	Leads restoration during incidents; documents lessons learned.
Business Owner(s):	Define critical data, sign off RTO/RPO; validate test restores.
Vendors/MSP:	Provide support for backup platform and cloud services; escalation contacts.

3. Data Inventory & Classification

3.1 Systems & Data Sets:

System / App	Data Type(s)	Business Criticality	Owner	RTO / RPO
Example: Microsoft 365 (Exchange, SharePoint, OneDrive, Teams)	Email, docs, sites, chat, recordings	High	Head of Operations	RTO: 8h / RPO: 4h

3.2 Classification:

Identify sensitive data (e.g., personal, financial, IP) and any legal/regulatory retention requirements.

Sensitive Data	Notes

4. Backup Strategy

Item	Completed Yes/No	Notes
4.1 Method: Follow the 3-2-1 (or 3-2-1-1-0) rule: 3 copies, 2 media types, 1 offsite; +1 immutable; 0 restore errors verified.		
4.2 Scope: Back up data, applications, and configuration (including SaaS like Microsoft 365, cloud workloads, and on-prem endpoints).		
4.3 Schedule: Define full/incremental schedules and retention (e.g., daily incrementals, weekly full, 90-day retention; monthly/quarterly archives).		
4.4 Security: Encrypt backups in transit and at rest; restrict access (RBAC); enable immutability / write-once storage; segregate backup admin accounts.		
4.5 Offline/Offsite: Keep at least one logically isolated (off-network) copy to resist ransomware.		

5. Technology & Configuration

Document tooling (e.g., Microsoft 365 backup solution, Azure Backup, Veeam, NAS/Tape, Object Storage). Include job names, policies, repositories, encryption keys management, and immutability settings.



6. Backup Jobs Catalogue

Job Name	Scope (systems/data)	Schedule	Retention	Storage Targets	Notes (immutability, encryption)
Example: M365 Backup – All Tenants	Exchange, SharePoint, OneDrive, Teams	Daily 22:00 (incremental); Weekly full Sunday	90 days; legal hold per site	Local NAS + Cloud object storage (immutable 14 days)	AES-256 encryption; RBAC restricted

7. Recovery Procedures

Item	Notes
7.1 Activation criteria: When to initiate restoration (e.g., ransomware detected, accidental deletion, outage).	
7.2 Decision flow: Choose restore level: file/item → workload/app → full system/VM → failover site.	
7.3 Step-by-step restore: Document commands/UI paths for common scenarios (mailbox restore, SharePoint site restore, VM instant recovery, database point-in-time).	
7.4 Validation: How to verify data integrity and business acceptance (checksum, application tests, user sign-off).	
7.5 Communication: Who to notify (internal stakeholders, customers, regulators); include templates.	

8. Testing & Verification

Plan and record tests at least quarterly. Include both technical verification and business validation. Use automated recovery verification where available.

Test ID	Scenario	Date	Result	Issues Found	Actions / Owner
T-001	Restore SharePoint site to alt location	___/___/___	Pass/Fail	—	—

9. Monitoring & Metrics

Item	Notes
Success rate of backup jobs (%) and failed jobs re-run time	
RPO achieved vs target; RTO achieved vs target	
Storage utilisation, retention compliance	
Restore test frequency and success	
Immutable/offsite copy status	

10. Security & Access Controls

Item	Notes
Backup admin accounts separated from domain/admin; MFA enforced	
Role-based access control; least privilege; audit logging	
Keys & secrets management (rotation policy)	
Network isolation for backup repositories; deny interactive logon	
Tamper protection and deletion hold for backup sets	

11. Vendor & Support Contacts

Vendor / Provider	Service / Product	Contract / SLA	Escalation Contact
Example: Backup Vendor Ltd.	Cloud-to-cloud M365 backup	SLA: 99.9%; support 24x7	support@vendor.com; +61 2 0000 0000

12. Plan Maintenance

Item	Notes
Review cadence (quarterly) and after significant changes	
Change log and versioning	
Training & awareness for staff	
Alignment with Business Continuity and Incident Response plans	

Appendix A: Quick Reference – 3-2-1-1-0 Backup Rule

- 3 copies (production + 2 backups)
- 2 different media or storage types
- 1 offsite/off-network copy
- +1 immutable (write-once) copy
- 0 errors (regularly tested restores)

Appendix B:

Sample Recovery Runbook (fill in commands/screenshots for your tools)

Appendix C:

Test Evidence Log (attach reports, screenshots, export from tooling)

References & Alignment

- ACSC Essential Eight – Regular Backups (controls for performing, securing, protecting, and testing backups).
- ISO/IEC 27031 – ICT readiness for business continuity (align ICT recovery with business continuity).
- NIST SP 800-34 – Contingency Planning Guide (ISCP process, BIA, recovery strategies).
- AWS Well-Architected Reliability – Back up data (RTO/RPO, automation, periodic recovery verification).
- Microsoft 365 Backup Best Practices – shared responsibility, retention, and SaaS recovery considerations.