



BACKUP & DISASTER RECOVERY PLANNING GUIDE

Keep essential services moving

For nonprofit, human-services and behavioral-health leaders. Spend about 45 minutes with operations and IT to define targets, identify missing evidence and schedule a test.

Use this guide: complete one worksheet for a priority service, then repeat for others. Fill the boxes digitally or print them. Store completed copies internally; include system names, not passwords or participant records.

Define the work before the technology

Name the service staff must deliver during an outage: coordinating a residential shift, reaching a clinic schedule, documenting a visit, or processing payroll. Decide what can safely wait and what temporary process staff will use.

Organization / service / accountable program lead

Minimum work that must continue; impact if it stops

RTO: the target time to restore a usable service.

RPO: the target maximum period of data loss. Both are planning targets to test, not promises from a successful backup job.

RTO target / RPO target / who approved these targets

Systems and dependencies needed first; approved temporary workflow



02 / CONFIRM COVERAGE

Know what can be restored

Ask your IT contact or provider to show current evidence. Choose Yes, Partial, No, Unknown or N/A. Record the reason for any N/A response in the notes.

Microsoft 365 workloads are explicitly covered

List protected mailboxes, SharePoint sites and OneDrive accounts. Ask separately about Teams, Planner and Forms data; do not assume every workload is included.

Google Workspace recovery is documented, if used

Confirm Gmail, My Drive and shared-drive coverage, recovery windows, deleted-user handling and who can restore. Retention or a recycle bin alone is not a full recovery plan.

Servers, file shares and SaaS applications are mapped

Include identity services, configurations, databases and vendor-hosted program systems. Document what the provider restores and what your team must rebuild.

Backup access and deletion are protected

Identify who can delete recovery copies, how privileged access is protected, and what copy remains usable after a compromised account or site outage.

Failures and exclusions receive follow-through

Name who checks backup alerts, the escalation deadline and where exceptions are recorded. Verify that newly added systems enter coverage.

Recovery can work without the usual workstation

Confirm access to runbooks, emergency contacts, recovery tools and credentials through an approved alternative path.

Uncovered data / retention window / responsible contact / evidence location



03 / PROVE THE RESULT

Test that staff can work

A suggested quarterly cycle: choose one service, perform an authorized test, record the outcome and close the gaps. Increase or change the cadence when service impact or major changes justify it.

Before the test

Agree scope, target times, a safe test environment, stop conditions and who can approve changes. During an incident, the incident lead must authorize recovery after assessing containment and trust.

During the test

Restore the chosen sample using verified recovery assets. Have authorized staff sign in and complete a representative task. Record dependencies, elapsed time and the age of recovered data.

After the test

Compare the result with the agreed targets. Check permissions and integrity, document manual-work reconciliation and assign corrective actions before closing the exercise.

Test date / service / scenario / participants

Measured restore time / actual data-loss window / staff task completed

Pass or fail against targets / evidence / unresolved exceptions

Next test date / responsible lead / retest trigger



04 / AGREE THE NEXT ACTIONS

Turn the findings into decisions

Use the first review to choose up to three changes that most improve continuity. A purchased backup product is one part of that work.

Priority 1: service gap / next action / responsible person / due date

Priority 2: service gap / next action / responsible person / due date

Priority 3: service gap / next action / responsible person / due date

Leadership acceptance / next review date / evidence folder

Suggested annual rotation: Q1 identity and communications; Q2 program records and files; Q3 finance and a critical vendor; Q4 a broader service exercise. Adapt the rotation to your dependencies and prior failures.

Reference guidance

[Microsoft: Microsoft 365 Backup overview](#)

[NIST: Cybersecurity Framework 2.0 - Small Business Quick-Start Guide](#)

Planning aid, not a full incident-response or disaster-recovery plan. Verify product coverage and recovery windows against your configuration. References reviewed September 8, 2026.

Bitralynx Solutions helps nonprofit teams map dependencies, manage backup coverage and validate service recovery.

Start with a complimentary Technology Readiness Review: one 45-minute conversation and a one-page list of practical priorities. [Book your review](#) or email info@bitralynx.com.