Small business backup and recovery plan

Use this worksheet to decide what you need back, how much work you can afford to lose and who will recover it. Start with essential data. Duplicate pages 2–4 for each system or data set. The last page is a fictional example, not a recommended configuration.

Business and plan owner

_____

Version date and next plan review

_____

Secure plan location and outage accessible copy

_____

1 Identify the work that depends on data

Include cloud accounts, invoices, appointments, customer records, email, project files and local devices. Name the person who can confirm the data is usable. Use priority 1 for the first service to restore.

Data or system and location	Business owner	Restore priority

Sensitive information: describe categories only. Do not put customer records, passwords, tokens, keys or recovery codes in this worksheet.

Set recovery expectations

Lost work target: the maximum age of recovered data you can tolerate. Downtime target: the longest acceptable interruption before the essential work resumes. These targets are separate; tests show whether your current approach can meet them.

Keep the completed plan restricted to authorized people. Make a secure copy available if your normal device or account is unavailable.

2 Plan the backups

Data or system name and business owner

_____

Included folders records and settings plus anything excluded

_____

_____

Acceptable lost work in minutes or hours and business reason

_____

Acceptable downtime in minutes or hours and business reason

_____

Backup tool or method and format

_____

Backup frequency and who checks success or failure alerts

_____

Retention period and how long older versions remain available

_____

Local copy location and protection

_____

Offsite copy location and protection

_____

Offline copy method and disconnect or rotation schedule

_____

Local is nearby; offsite is elsewhere; offline is disconnected. Record any gap. Encrypt sensitive backups and protect access. Match frequency and retention to your work, risks and any applicable recordkeeping requirements.

3 Write the recovery steps

Data or system name and restore priority

_____

Responsible person backup person and support contact

_____

Required device software versions licenses storage and network

_____

_____

Secure separate access instructions location and authorized custodian

_____

Record where approved access instructions are held and who can use them if the usual account or device is unavailable. Never write passwords, tokens, encryption keys or recovery codes here. Keep those in approved secure storage, separate from this plan.

Step 1 Confirm the incident and choose a known usable backup

_____

Step 2 Prepare a clean authorized recovery destination

_____

Step 3 Retrieve the backup and follow the product restore procedure

_____

Step 4 Check records and essential workflows with the business owner

_____

Step 5 Record who approves return to service and how to switch safely

_____

If compromise is suspected, involve qualified support before reconnecting systems or restoring. Preserve evidence and avoid bringing infected data or systems back into service.

4 Test and record the results

Restore to an isolated, safe test location. Never overwrite production data. Restrict access to sensitive records, disable live integrations and notifications, and securely remove temporary test copies when approved. A small test does not validate full business recovery.

System test owner and test date

_____

Scenario scope sample records and isolated destination

_____

Simulated loss time and restored backup timestamp including time zone

_____

Measured age of recovered data versus acceptable lost work target

_____

Start time end time and total recovery time including validation

_____

Downtime target and whether the measured test met it

_____

Checks performed completeness readability and essential workflows

_____

_____

Pass fail or limited result and what was not tested

_____

Problems corrective action owner and due date

_____

Next test date and triggers for earlier retesting

_____

Retest after important changes to data, software, access or the backup method. Record observed results honestly; a successful test is not a recovery guarantee.

Fictional filled example

Maple Lane Design is an invented two-person business. All people, systems, dates and results below are illustrative. This example covers project files only, not the entire business.

Data and targets

Project folder on the studio workstation; owner and recovery lead: Alex, studio owner. Backup person: Jo, studio manager. Priority 1. Acceptable lost work: 24 hours. Acceptable downtime: four hours.

Backup arrangement

Nightly encrypted, versioned backup to an offsite service with 90-day retention. Each Friday, copy to an encrypted rotating drive, disconnect it and store it at a separate secure location. Keep eight weekly copies. Alex checks daily completion and failure alerts. A cloud account outage could require using the older offline copy and exceed the lost-work target.

Access and prerequisites

Use a clean spare laptop with the licensed design software, matching fonts and enough storage. Jo holds the support contact in the restricted contact directory. Authorized staff retrieve credentials and drive recovery information through the separate approved vault and its emergency-access procedure; no secrets are stored in this plan.

Restore procedure

Confirm scope with Alex; select the last known usable backup; prepare an isolated test folder on the spare laptop; restore a sample project using the backup tool; open the design and linked assets; compare record counts and recent changes. Alex approves any real return to service after support confirms it is safe.

Measured test result

Test: 12 October 2026. Simulated loss: 10 a.m.; selected backup: 11 p.m. the prior day, both local time. Recovered data was 11 hours old, within the 24-hour target. Restore and validation ran 10–10:42 a.m., 42 minutes, within the four-hour target for this sample only. Three project folders opened; a missing font required installation. Full recovery and offline fallback were not tested.

Follow through

Jo will add the font prerequisite by 16 October. Next test: 12 November 2026, including the offline copy and a larger project set. Securely remove test copies after review. The test does not prove the whole business can recover within four hours.

Sources

1. CISA StopRansomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

2. CISA Protect data stored on your devices
https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices

3. NIST Recovery Point Objective
https://csrc.nist.gov/glossary/term/recovery_point_objective

4. NIST Recovery Time Objective
https://csrc.nist.gov/glossary/term/recovery_time_objective

5. NIST Small Business Information Security
https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf