

Backup & Ransomware Recovery Playbook

Build Backups That Survive Hardware Failure, Accidental Deletion, and Ransomware

Backups are not paperwork.

They're the difference between a bad day and losing years of photos, documents, financial records, family history, and everything else your computer was quietly holding hostage for you.

The Grumpy Sysadmin

Version: August 2026

SAMPLE
thegrumpysysadmin.com · full version has 18 pages

How to Use This Playbook

This playbook is designed for ordinary Windows users who need a backup system they can understand, maintain, and actually recover from. The goal isn't to turn your house into a data center. The goal is to keep one failed drive, one bad click, or one ransomware infection from becoming permanent.

Work through the design sections first, then the protection and testing sections, and finally the ransomware response plan. Fill out the worksheets and keep a copy somewhere other than the computer they describe.

Grumpy Rule: The disaster isn't the day to discover what your backup software meant by "retention policy."

The Five Questions Every Backup Plan Must Answer

- What data would hurt to lose?
- How many independent copies exist?
- Can the protected computer modify or destroy every backup?
- How far back can you restore?
- Have you successfully restored anything?

Table of Contents

- 1. Decide What Must Be Protected
- 2. Build a 3-2-1 Backup Design
- 3. Cloud Backup, Cloud Sync, Local Drives, and NAS
- 4. Add Ransomware-Resistant Protection
- 5. Protect Backup Accounts and Credentials
- 6. Set Retention and Recovery Points
- 7. Test Restores Before You Need Them
- 8. Ransomware: The First Hour
- 9. Decide Whether the Computer Can Be Trusted
- 10. Rebuild and Restore in the Right Order
- 11. Recovery Priorities
- 12. Backup Inventory and Emergency Worksheets
- 13. Maintenance Schedule
- 14. Final Verification

1. Decide What Must Be Protected

Start by separating irreplaceable data from replaceable software. Windows can be reinstalled. Most applications can be downloaded again. Your family photos, tax records, manuscripts, financial files, and twenty years of personal documents are a different story.

Grumpy Rule: *Back up what would make you swear the loudest if it vanished.*

Classify the Data

Data Inventory	Done
Documents and personal records	☐
Photos and videos	☐
Financial/tax records	☐
Email stored locally	☐
Browser profiles/bookmarks if not otherwise synchronized	☐
Password-manager emergency/recovery information	☐
Creative projects and business files	☐
Virtual machines, databases, or specialized application data if applicable	☐
Device configuration or export files that would be painful to recreate	☐

Replaceable vs. Irreplaceable

Don't waste your best backup storage on things you can recreate in fifteen minutes while leaving irreplaceable data unprotected. Installers, game downloads, and temporary files usually rank below personal records and original content.

Create a recovery priority list

Mark your data Tier 1, Tier 2, or Tier 3. Tier 1 is what you need first after a disaster. Tier 2 matters, but can wait. Tier 3 is replaceable or low priority. You'll use these priorities during recovery.

2. Build a 3-2-1 Backup Design

A useful baseline is the 3-2-1 model: keep three copies of important data, use at least two storage locations or types, and keep one copy offsite or otherwise separated from the main system. For ransomware, the important part isn't the slogan. It's making sure one compromise cannot destroy every copy.

Grumpy Rule: *Three folders on the same drive aren't three backups. They're three opportunities for the same drive to disappoint you.*

A Practical Home-User Example

Example Design	Done
Copy 1: Working files on the computer	☐
Copy 2: Automatic local backup to an external drive or NAS	☐
Copy 3: Offsite/cloud backup with version history	☐
One local or cloud copy is protected from easy deletion or encryption	☐
Important data has more than one historical recovery point	☐

You don't have to use this exact arrangement. You do need independent failure domains. A power surge, theft, ransomware event, account compromise, or accidental deletion shouldn't be able to take out every copy at once.

Frequency: How Much Work Can You Lose?

Backup frequency should be based on how much recent work you can tolerate losing. If losing a week of work is unacceptable, a weekly backup isn't enough.

- Frequently changing critical files: protect daily or continuously through a real backup/versioning system.
- Photos and personal archives: back up after meaningful additions, not just once a year.
- System images: useful before major changes and periodically, but they shouldn't replace file-level backups.
- Disconnected archives: update on a schedule you can realistically maintain.

3. Cloud Backup, Cloud Sync, Local Drives, and NAS

These tools solve different problems. The safest design usually combines more than one of them.

Cloud Sync

Services that synchronize files between devices are excellent for convenience and can provide version history or deleted-file recovery. But synchronization is designed to propagate changes. If a bad change is synchronized everywhere, you're depending on the provider's versioning and retention to undo it.

Grumpy Rule: A second synchronized copy is helpful. A synchronized mistake is still a mistake with excellent distribution.

Cloud Backup

A dedicated cloud backup service is designed around historical recovery rather than simply keeping folders synchronized. Evaluate retention, version history, ransomware recovery, MFA, encryption, restore options, and what happens when a file is deleted from the original computer.

External Drives

External USB drives are inexpensive, fast, and simple. Their weakness is that a drive permanently connected and writable by the infected computer may be reachable by ransomware. A rotating or disconnected drive can provide valuable separation.

- Label the drives clearly.
- Use at least two drives if you want to rotate one offline.
- Encrypt the drive if loss or theft would expose sensitive information.
- Don't assume a drive is healthy because it still appears in File Explorer.
- Replace aging or unreliable drives before they become the emergency.

NAS

A NAS can provide excellent centralized storage, snapshots, and backup targets, but a shared folder mounted with broad write access can also become another place ransomware reaches. Use separate backup accounts, least-privilege access, snapshots/versioning, and protected backup features where supported.