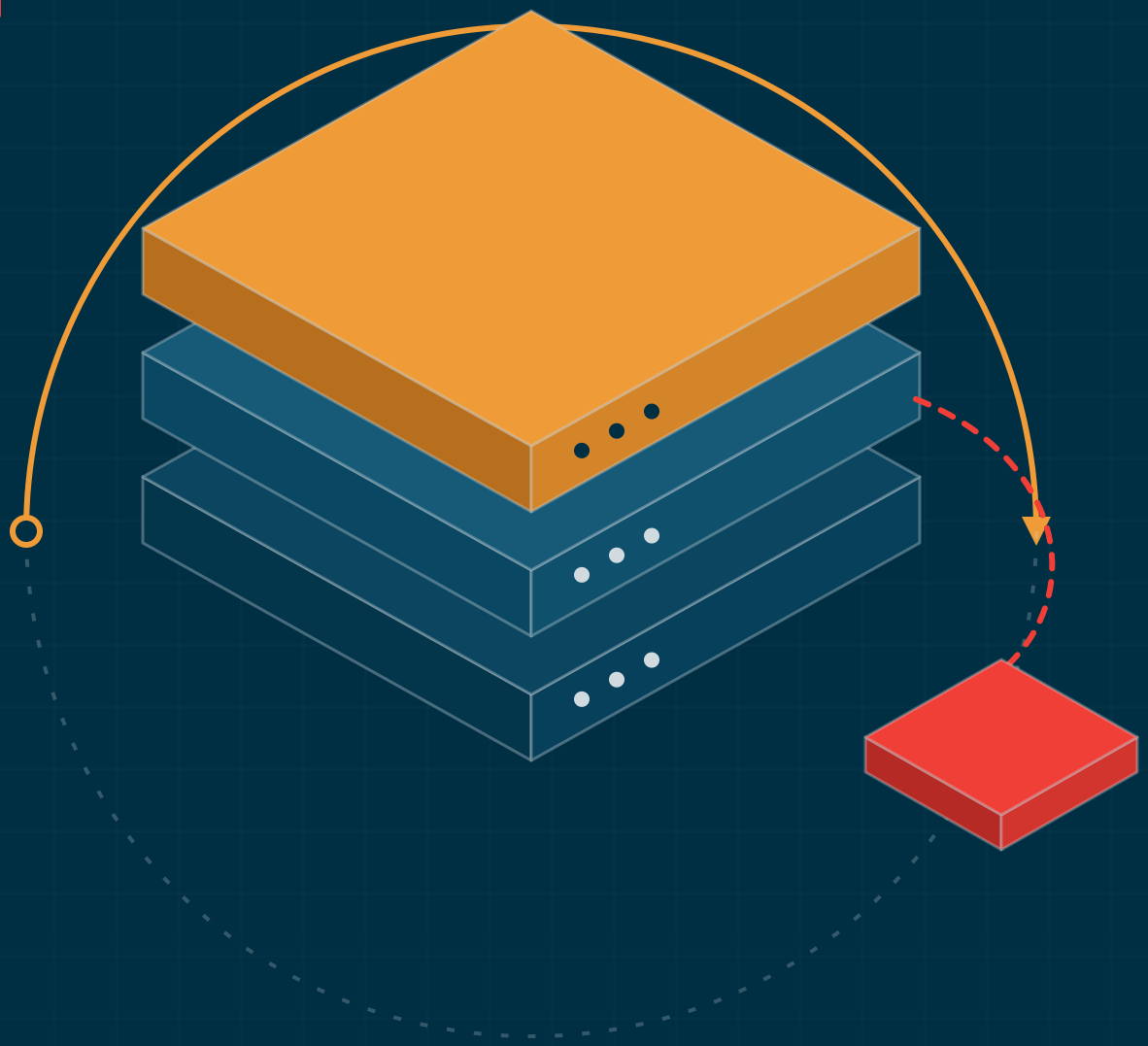
FREE GUIDE

PLANNING GUIDE



3
COPIES

2
MEDIA

1
OFFSITE

Backup & Disaster Recovery Planning Guide

How to make sure your business can bounce back

CMIT Solutions · Tri-City & Flint, MI

Saginaw · Bay City · Midland
Flint · Frankenmuth

BEFORE YOU START

Who this guide is for

This guide is for owners and managers of small and mid-sized businesses who want an honest answer to one question: if our data or systems disappeared tomorrow, how quickly could we get back to work?

You don't need to be technical. Each section ends in practical steps you can work through with your team or IT provider. By the end, you'll know what to protect, how fast you need it back, how to back it up and how to prove your plan works.

What can go wrong

Hardware failure

Drives, servers and laptops wear out, often without warning.

Ransomware

Malicious software can encrypt your files, and any backups it can reach.

Human error

An accidentally deleted folder or an overwritten spreadsheet.

Theft or loss

A laptop left in a car, or equipment taken from the office.

Site disasters

Fire, flooding, a burst pipe in a Michigan February or a long power outage.

Cloud account problems

A compromised or misconfigured account can change or delete data everywhere it syncs.

KNOW THE DIFFERENCE

Backup is a copy of your data. **Disaster recovery** is the plan, people and tools that get your business running again using that copy. You need both. A perfect backup with no plan can still leave you closed for longer than you can afford.

SECTION 1

Know what you need to protect

You can't recover what you didn't know you had. Start with a simple inventory of the systems and data your business runs on.

- ☐ **List your critical systems.** Accounting, line-of-business software, email, shared files, phone system, website and anything else your team uses daily.
- ☐ **Note where each one lives.** An office server, a specific desktop, a cloud service or a system hosted by a vendor.
- ☐ **Don't assume cloud apps are backed up.** Check what each provider actually keeps, for how long, and how you would restore it. Consider a separate backup for cloud email and files.
- ☐ **Find the files saved locally.** Desktops and laptops often hold documents that never made it to the shared drive.
- ☐ **Record what it takes to rebuild.** Software installers, license keys, configuration notes and vendor support contacts, with passwords kept in a secure vault.
- ☐ **Name an owner for each system.** The person who knows how it's used and can confirm that a restore actually worked.

> TRY THIS
>
> Ask each department: **"If you lost one system for a day, which would hurt most?"** The answers will shape the priorities you set in the next section.

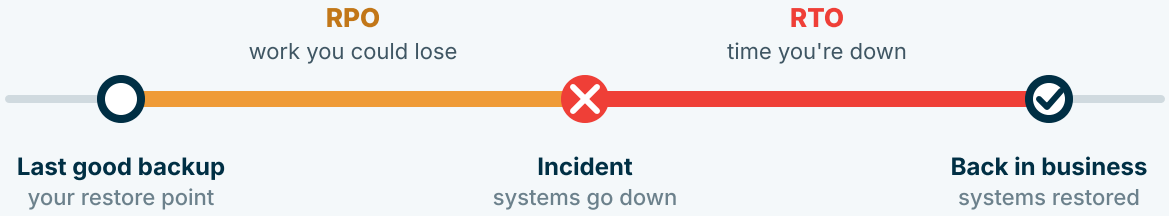
Inventory worksheet

System or data	Where it lives	Owner	Backed up?
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

SECTION 2

Set your recovery targets: RPO & RTO

Two simple measures turn "we need it back fast" into a plan you can build and budget for.



RPO

Recovery Point Objective

How much data, measured in time, you can afford to lose. If you back up only overnight, a failure in the afternoon could cost most of a day's work.

RTO

Recovery Time Objective

How long a system can be down before the impact on customers, staff or revenue becomes serious.

Recovery targets worksheet

System	What depends on it	RPO	RTO	Priority
Example: accounting	*Invoicing, payroll*	*A few hours*	*Next business day*	*High*
Example: shared files	*Daily work, quotes*	*One hour*	*Same day*	*High*

Examples are for illustration only. Your targets depend on how your business works.

Tighter targets usually require more capable solutions and cost more, so set them system by system rather than across the board.

SECTION 3

Build backups that hold up

The 3-2-1 approach is a simple, widely used rule of thumb for making sure no single failure can take out every copy of your data.

3
copies of your data
the original plus two backups



2
types of storage
e.g. local device + cloud



1
copy offsite
away from your building



+ Keep at least one copy offline or immutable (it can't be changed or deleted for a set period)

Make your backups dependable

- [ ] **Automate everything.** Nobody should have to remember to start a backup.
- [ ] **Encrypt backup data** both while it's moving and where it's stored.
- [ ] **Protect backup access** with separate credentials and MFA, so one stolen password can't erase your safety net.
- [ ] **Monitor every job.** Failures should alert a person who follows up, not just write to a log.
- [ ] **Keep enough history.** Set retention so you can go back to before a problem started, even if nobody noticed it right away.
- [ ] **Back up whole systems, not just files,** for servers and critical machines, so you can rebuild faster.

WATCH OUT

File sync is not the same as backup. If a file is deleted or encrypted on one device, a sync service can copy that change everywhere. A true backup keeps earlier versions you can go back to.

SECTION 4

Write the plan, then test it

A disaster recovery plan is the written answer to "what do we do now?" Keep it short enough that people will actually use it under pressure.

Your plan should cover

- [ ] **Who can declare a disaster** and approve emergency spending.
- [ ] **An offline contact list:** staff, IT provider, insurer, bank and key vendors.
- [ ] **Recovery order,** based on the priorities you set in Section 2.
- [ ] **Step-by-step restore procedures** for each critical system.
- [ ] **Where people will work** if the office is unavailable.
- [ ] **Ready-to-send messages** for staff, customers and vendors.

Your testing routine

- [ ] **Restore sample files** on a regular schedule, such as monthly.
- [ ] **Test a full system recovery** at least once a year.
- [ ] **Run a tabletop exercise:** talk through a scenario as a team.
- [ ] **Time your restores** and compare them with your RPO and RTO targets.
- [ ] **Update the plan** after new systems, staff changes or an office move.
- [ ] **Keep printed copies** where you can reach them during an outage.

THE GOLDEN RULE

A backup you haven't restored is a guess. Testing is the only way to know your backups work, and to learn how long recovery really takes before you need it for real.

KEEP IT CURRENT

Put a recurring reminder on the calendar to review the plan. An out-of-date contact list or a missing system can slow everything down on the worst day.

NEXT STEPS

How CMIT Solutions of Tri-City and Flint can help

Backups are easy to set up and easy to forget. Recovery is where planning pays off.

CMIT Solutions of Tri-City and Flint is a locally owned managed IT provider based in Frankenmuth and led by owner Linton Pinnock. We help small and mid-sized businesses across Saginaw, Bay City, Midland, Flint, Frankenmuth and the surrounding Mid-Michigan area protect their data and plan for recovery.

Review what you have

Look at your current backups, what they cover and what they miss, and explain the gaps in plain English.

Design around your targets

Build a 3-2-1 backup approach matched to the RPO and RTO you need for each system.

Monitor and manage

Keep an eye on backup jobs and follow up when something fails, so problems don't sit unnoticed.

Test and document

Run test restores and help you write, and keep updating, a disaster recovery plan your team can follow.

LOCAL TEAM, NATIONAL NETWORK

As part of CMIT Solutions, a network of 250+ locations across North America, we combine local, face-to-face service with the resources and shared experience of a larger organization.

How quickly could you recover?

Reach out through our contact page to talk through your plan.
cmitsolutions.com/tri-city-flint-mi-1251/contact-us/

CONTACT US

CMIT SOLUTIONS OF TRI-CITY AND FLINT

Practical IT and security support for Mid-Michigan businesses

OFFICE

CMIT Solutions of Tri-City and Flint
1055 S Main Street, Suite A
Frankenmuth, MI 48734

SERVICE AREA

Saginaw, Bay City, Midland, Flint, Frankenmuth and surrounding Mid-Michigan communities

GET IN TOUCH

https://cmitsolutions.com/tri-city-flint-mi-1251/contact-us/

OWNER

Linton Pinnock
Locally owned and operated

CMIT Solutions · Tri-City & Flint, MI



This guide offers general information and best practices. It is not legal, insurance or compliance advice. © 2026 CMIT Solutions of Tri-City and Flint.