

ProtectIT Management

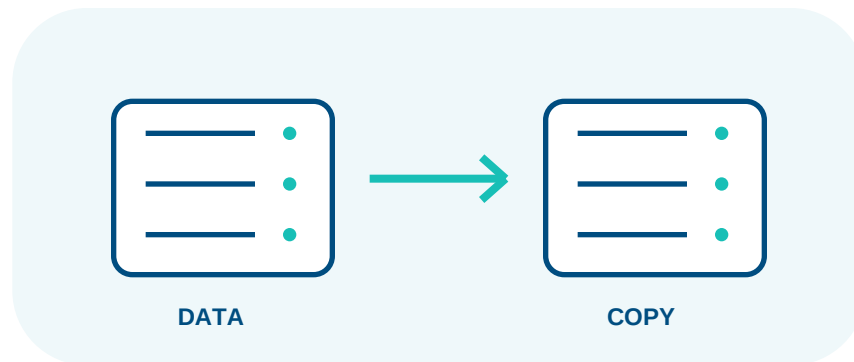


Backup & Recovery Guide

Practical Protection Without the Overwhelm

One smart action at a time.

Why Backups Matter



A backup is a separate copy of important business data that can be used when the original data is lost, damaged, deleted, encrypted, or otherwise unavailable.

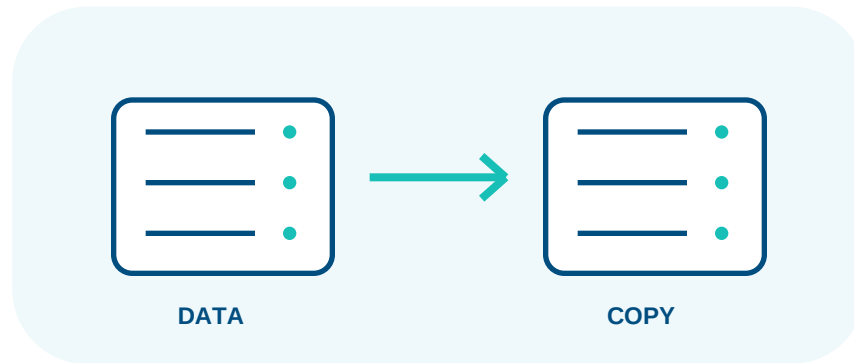
Common causes of data loss

- *Ransomware or cyberattack*
- *Accidental deletion*
- *Hardware failure*
- *Lost or damaged devices*
- *Account compromise*
- *Software or system failure*

BACK UP • PROTECT • RECOVER

A backup is only useful if you can restore from it.

How to Protect Your Business



- ✓ *Identify the information your business cannot operate without.*
- ✓ *Back up critical information regularly.*
- ✓ *Keep backup copies separate from primary systems.*
- ✓ *Protect backup accounts with strong authentication and limited access.*
- ✓ *Monitor whether scheduled backups actually complete.*
- ✓ *Know who is responsible for backups and recovery.*
- ✓ *Test that important information can actually be restored.*

If Important Data Is Lost or Unavailable

- *Stay calm and avoid uncontrolled changes.*
- *Contact your IT provider or responsible technical team.*
- *Determine which systems and data are affected.*
- *Avoid overwriting or deleting potentially recoverable information.*
- *Follow your organization's recovery process.*
- *Document what happened and what was recovered.*

Technical Measures That Improve Recovery

Business Practices

- ✓ *Establish a documented backup schedule.*
- ✓ *Identify critical systems and information.*
- ✓ *Assign responsibility for reviewing backup status.*
- ✓ *Maintain a documented recovery plan.*

Technical Controls - IT Managed

- ✓ *Maintain separate, protected backup copies.*
- ✓ *Use offline or immutable backup protection where appropriate.*
- ✓ *Restrict administrative access to backup systems.*
- ✓ *Monitor backup jobs and failures.*
- ✓ *Test restoration procedures periodically.*
- ✓ *Document recovery objectives for critical systems.*

Backup ≠ Recovery

Backup: *Do we have another copy?*

Recovery: *Can we restore what the business needs when it needs it?*

ProtectIT Recommendation

Small businesses depend on access to their data and systems to serve customers and continue operating.

Backups are an important safeguard, but simply having a backup does not guarantee that the business can recover when something goes wrong.

Work with your IT provider or MSP to understand:

- ✓ *What is being backed up?*
- ✓ *How frequently do backups occur?*
- ✓ *Where are backups stored?*
- ✓ *Who has access to them?*
- ✓ *How long could recovery take?*
- ✓ *When was recovery last tested?*

ProtectIT Management helps organizations reduce human cybersecurity risk by strengthening employee awareness, behavior, and visibility—working alongside existing IT and security providers, not replacing them.

Want to Strengthen Your Cybersecurity Readiness?

Schedule a free cybersecurity risk discussion.

www.protectitmngmt.com

info@protectitmngmt.com