Fact sheet

Backups – Prepare for an emergency

What is a backup

A backup is a copy of all your important data that is stored separately from the original. If your primary files are lost due to accidental deletion, hardware failure, theft, or cyber incident, backups allow you to restore your information quickly and continue working with minimal disruption.

Backups can include:

- work documents and shared files
- emails and communications
- photos and videos
- system files and applications
- databases and business information
- personal records and important documents.

Why are backups essential

Data loss can happen at any time and often when least expected. Devices fail, systems crash and cyber incidents can disrupt access to important information.
Even a simple mistake like saving over a file or deleting the wrong folder can lead to permanent data loss.

Without a backup, recovering lost data can be difficult, costly, or impossible. With a proper backup in place, recovery can take minutes instead of days. Backing up your data is one of the simplest and most effective ways to protect your organisation's information and your personal information.

Some common causes of data loss include:

- accidental deletion or human error
- hardware or device failure
- lost or stolen devices
- software corruption
- malware or ransomware attacks and other cyber attacks
- natural disasters or physical damage.

Ways to backup data

There are several ways to back up your data. Using a combination of methods provides the strongest protection.

- **Cloud-based products**

Cloud backup services store your files securely online and automatically synchronise changes. Cloud backups are ideal for documents, collaboration files, and frequently updated information.

Benefits

- access from anywhere
- automatic backups
- protection from device loss or damage
- easy recover options.

- **External or physical hard drives**

External hard drives and solid-state drives (SSDs) provide physical backup storage. Physical backups are useful for large files, archives, and data that requires offline protection.

Benefits

- large storage capacity
- fast backup and recovery
- one-time purchase cost
- can be stored offline for additional security.

- **Network or shared drives**

Share drives and network-attached storage solutions are often used within organisations to centrally store and protect business data.

Benefits

- centralised storage
- shared access for teams
- scheduled automatic backups
- managed security and access controls.

The 3-2-1 backup rule

One of the most effective ways to protect your data is by following the 3-2-1 backup rule:

- 3 copies of your data (1 original + 2 backups)
- 2 different storage types (example: cloud and an external drive)
- 1 copy stored offsite or offline.

This approach helps ensure that even if one backup fails, is lost, or becomes inaccessible another secure copy is still available for recovery.

The impact of not backing up

Data loss is more than an inconvenience - it can disrupt operations, damage stakeholder trust, and result in significant financial and reputational consequences.

Without reliable backups in place, businesses and organisations may experience:

- loss of critical work, records, or project files
- operational disruption and extended downtime
- financial losses and reputational damage
- compliance and regulatory risks
- increased stress and recovery costs.

Cyber incidents such as ransomware make backups even more critical. In the event of an attack, a secure and up to date backup can enable systems and data to be restored quickly, reducing downtime and limiting business impact.

Backups are a fundamental part of cyber resilience and business continuity. They help ensure that when incidents occur, recovery is possible, and disruption is minimised.