# DATA BACKUP AND DISASTER RECOVERY PLAN

## When disaster strikes, business suffers.

Having a robust data backup and IT disaster recovery plan (DRP) is critically important to maintain business continuity.

The costs of not having an IT DRP are severe:

- £ Prolonged business interruption
- £ Increased operating costs
- £ Complete data loss
- £ Negative publicity and reputational damage
- £ Lost customers
- £ Legal fees
- £ Repairing IT systems
- £ Regulatory penalties.

# Always have a backup plan

- ✓ Set clear recovery objectives for your plan.
- ✓ Conduct risk assessment and business impact analysis.
- ✓ Establish minimum equipment needs to get you back up and running.
- ✓ Document the processes and procedures of your DRP.
- ✓ Keep a copy of your DRP offsite and secure.
- ✓ Ensure that every member of staff knows what they should do if disaster strikes.

Decide what data you want to backup based on its importance to your business and the level of risk.

Automate your data backups (ensure the system is configured to notify you if the backup fails).

Bad things happen to good backups. Files get corrupted for many different reasons. Configure your backups to ensure the integrity of data for recovery.
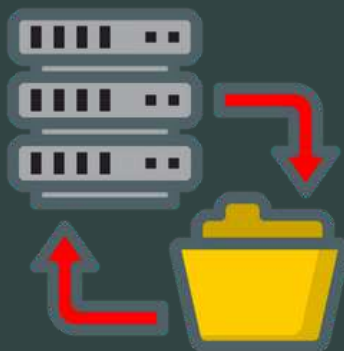
Decide how long you need to keep backup data, and when it should be permanently deleted.

GDRP requires organisations take suitable precautions to protect backup systems and ensure the timely recovery of data after an incident.

Backup your data frequently. Data files that are constantly in use will need backing up more often.

## FOLLOW THE RULE OF

# 3

Keep 3 copies of your data

Keep 2 copies on different storage media

Keep 1 copy in a different physical location.

- ✓ Security matters. Use encryption to keep your backup data secure and restrict access to it.
- ✓ Run data restoration tests regularly to ensure the backup is working correctly and accurately.
- ✓ Ensure your install the latest backup software updates, upgrades and security patches.
- ✓ Review your backup requirements, systems and DRP regularly.