Backup Policy Template for UK Small Businesses

Backup Policy Template

We know that a backup is useful only if the organisation can recover the information Backup needs. Hardware failure, deletion, ransomware and service disruption can all affect access to business data.

A Backup Policy records what must be backed up how often copies are made how they are protected and how the organisation checks that restoration works.

1. Define Your Backup Requirements

Complete this table for the systems your business actually uses.

System or data	Required backup coverage	Frequency	Retention
Shared business files	[Define folders and data]	[Set schedule]	[Set period]
Business applications and databases	[Define required data]	[Set schedule]	[Set period]
Servers or virtual machines	[Define systems and configurations]	[Set schedule]	[Set period]
Microsoft 365 or other cloud services	[Confirm service coverage]	[Set schedule]	[Set period]
Critical configuration files	[List required configurations]	[Set schedule]	[Set period]

Do not assume that every cloud service automatically provides the exact independent backup and restoration arrangements your business requires. Check the capabilities of each service. Document any gaps.

2. Backup Protection Rules

The organisation must define controls to protect copies from accidental deletion, unauthorised access and incidents affecting the main environment.

Recommended areas to assess include:

- Restricting access to backup consoles and stored copies.
- Protecting administrator accounts.
- Using encryption where appropriate.
- Monitoring backup jobs and investigating failures.
- Keeping an otherwise protected copy where appropriate to the risk.
- Documenting retention and secure deletion requirements.
- Testing recovery than relying solely on successful backup notifications.

3. Backup Policy. Copy-Ready Statement

Policy owner: [Insert role]

IT contact: [Insert contact]

Review date: [Insert date]

We must identify business information and systems that require backup protection. Backup schedules and retention periods must be defined according to business requirements, recovery priorities and applicable obligations.

The IT team or appointed service provider must monitor operations investigate failures and maintain records of significant issues. Access to backup systems must be restricted to authorised personnel.

We must test restoration periodically to confirm that selected data and systems can be recovered and used. Test results, problems and corrective actions must be documented.

When a data-loss or cyber-security incident occurs recovery must follow the incident-response and disaster-recovery procedures. Before restoring data after a suspected cyberattack the response team must assess whether the chosen backup and recovery environment are safe to use.

Any exception to this policy must be approved by [authorised role] and recorded. The policy must be reviewed periodically and when backup systems, business requirements or recovery priorities change.

4. Backup Failure: Response Process

1. **Detect the problem:** Review alerts or reports to identify whether a backup failed, was incomplete, or did not run as expected.
2. **Assess the impact:** Identify the affected system, the last successful backup, and the period of data that may be at risk.
3. **Resolve the cause:** Investigate and fix issues such as insufficient storage space, network connectivity problems, incorrect permissions, or service errors.
4. **Confirm a successful backup:** Run the backup again and verify that it has completed successfully. Record any period during which data was not adequately protected.
5. **Escalate if necessary: I**nform the responsible manager if critical systems remain unprotected or the organisation's recovery requirements may not be met.

If the failure is associated with suspected ransomware or unauthorised access follow the security incident procedure rather than treating it as an ordinary backup error.

5. Backup and Restore Test Checklist

- Select a system or data set.
- Confirm that an appropriate backup copy exists.
- Record the recovery point being tested.
- Restore to a test location where possible.
- Verify that the restored data is readable and usable.
- Check whether the restored system meets the test objective.
- Record the time taken and any errors.
- Assign corrective. Retest where needed.

6. Backup Policy Review

Review backup coverage whenever a new business application is introduced when important data moves to a location or when recovery needs change.

Keep the completed schedule the people responsible, the test records and any exception approvals with the approved policy.

Related Resources

Read our Disaster Recovery Plan Template for SMEs to see how backups fit into recovery arrangements. You can also browse the Free IT Policy Templates, for UK Businesses hub.

Disclaimer: Complete the schedules. Confirm your actual backup capabilities before using this template. It does not guarantee that your data can be recovered in every situation.