[Company name]

How to use this document: delete this paragraph before saving, sharing, or circulating it. Every part shown in blue is yours to replace: type your own details over each blue [field] until no blue remains. Then select all (Ctrl+A) and set the font colour to the same dark colour throughout. What is left is your finished document.

IT Backup Checklist

A recurring check that backups ran, are stored safely, and can actually be restored.

1. Checklist details: Backup period covered by this checklist: _____ **Person completing this checklist:** _____

Role of the person completing this checklist: _____ **Date this checklist was completed:** _____

Backup system or service in use: _____

2. Scope: what must be backed up: [ ] Every system and data store that the business depends on is listed in the backup scope, including file storage, email, databases, and any hosted services.

[ ] Each item in scope has a named owner who is responsible for confirming its backups.

[ ] New systems added since the last review have been added to the backup scope before this checklist was signed off.

[ ] Systems no longer in use have been removed from the scope and their old backups handled under the retention rules.

[ ] The backup scope covers data held by outside providers as well as data held on local equipment, where that applies.

3. Daily checks: [ ] The most recent scheduled backup job completed without errors, or every error has been recorded in section 6.

[ ] The size and duration of the most recent backup are consistent with recent backups, and any unusual change has been investigated.

[ ] Backup failure alerts are switched on and were received by the person on duty, not only recorded in a log nobody reads.

[ ] Storage used by backups is within capacity, with enough free space for the next scheduled backup.

[ ] Any backup job that was skipped, paused, or run manually is noted, with the reason, in section 5.

4. Weekly checks: [ ] At least one backup copy is held away from the main site or in a separate hosted location, so a single site problem cannot destroy both the original data and its backup.

[ ] Backup copies are protected so that only authorised people can read, change, or delete them.

[ ] Encryption is switched on for backup copies that hold sensitive information, and the recovery keys are stored separately from the backups themselves.

[ ] Retention rules have been applied: backups older than the agreed retention period have been deleted or archived as the rules require.

[ ] The backup schedule still matches how often each system changes, and the recovery point objective for each critical system is still achievable.

5. Restore testing: [ ] A restore has been tested in this period from a recent backup, not only from the backup software's own success message.

[ ] The restored data was opened and checked, and the check confirmed it was complete and usable.

[ ] The time taken to restore was recorded and compared with the recovery time objective for that system.

[ ] Any restore that failed, or took longer than the objective, has an agreed fix and a retest date in section 6.

[ ] The restore test covered a different system or data set from the previous test, so testing rotates across the estate over time.

6. Backup log Record each backup job in this period. Add or remove rows to fit the number of jobs.

Date of the backup	System or data backed up	Type of backup performed	Result of the backup job	Checked by

7. Failure and follow-up log Record every failure, missed job, or restore problem, the action taken, and the date it was closed.

[Company name]

Date the problem was found	System affected	Description of the problem	Action taken	Date closed

8. Sign-off By signing, the person below confirms the checks above were actually carried out, and that every open failure in section 7 has an owner and a date for closure.

Checker name: _____ **Reviewer name:** _____

Checker signature: _____ **Reviewer signature:** _____

Date of sign-off: _____