Backup and Data Verification Checklist for Small Businesses (2026 Edition)

This checklist helps you confirm your backups are not just running—but actually working.

Backup and Data Verification Checklist

1. Confirm Backups Exist for All Critical Systems

- ☐ Computers and laptops are backed up
- ☐ Servers (if any) are backed up
- ☐ Mobile devices used for work are backed up
- ☐ Cloud systems (Microsoft 365, Google Workspace) are included

Why this matters:
If it's not backed up, it will be lost eventually.

2. Use the Right Type of Backup (Not Just Sync)

- ☐ Backup solution stores independent copies of data
- ☐ Cloud sync tools (OneDrive, Google Drive, Dropbox) are not treated as backups
- ☐ Backup system protects against deletion and ransomware

Why this matters:
File sync is not a backup. Deleted or encrypted files can sync instantly across devices.

3. Ensure Backups Run Automatically

□ Backups are scheduled (not manual)
□ Backup frequency matches business needs (daily or more often)
□ Backup failures are visible and addressed

Why this matters:
Manual backups are inconsistent and unreliable.

4. Maintain Offsite or Cloud Backup Copies

□ At least one backup is stored offsite or in the cloud
□ Backups are not only stored on the same device or network
□ Backup storage is protected from ransomware

Why this matters:
Local-only backups can be destroyed along with your systems.

5. Verify Backup Success Regularly

□ Backup logs are reviewed
□ Last successful backup date is known
□ Errors or skipped files are investigated

Why this matters:
Backups can fail silently if no one is checking them.

6. Perform Test Restores (Critical Step)

□ Random files are restored successfully
□ Full restore capability is tested periodically
□ Recovery process is documented

Why this matters:
If you cannot restore your data, your backup is not working.

7. Validate Backup Storage Devices

□ External drives open and function correctly
□ No signs of hardware failure
□ Drives are replaced when aging or unreliable

Why this matters:
Backup hardware can fail just like primary devices.

8. Protect Backup Access and Credentials

□ Backup systems require secure login
□ Access is limited to authorized users
□ Backup credentials are not shared or reused

Why this matters:
If attackers access your backups, they can delete or encrypt them.

9. Understand Backup Limitations

□ You know what is included in backups
□ You know what is NOT included
□ Recovery time expectations are clear

Why this matters:
False assumptions about backups are a major business risk.

10. Avoid Relying on Free or Personal Backup Tools for Business

□ Business data is not dependent on consumer-only backup tools
□ Backup solution includes monitoring and alerts
□ Backup system supports business continuity

Why this matters:
Free tools lack monitoring, ransomware protection, and validation features needed for business environments.

11. Secure and Store Backup Media Properly

□ Backup drives are stored safely
□ Physical access is controlled
□ Drives are not left connected unnecessarily

Why this matters:
Improper storage can lead to data loss or theft.

12. Align Backup Strategy with Business Needs

□ Critical data is prioritized
□ Backup frequency matches operational importance
□ Recovery objectives are defined

Why this matters:
Not all data needs the same level of protection—but critical data must be recoverable quickly.

What a Reliable Backup System Looks Like

Backups run automatically
Data is stored in multiple locations
Restores are tested regularly
Backup failures are identified and fixed quickly

Quick Rule of Thumb

Backups don’t protect your business.
Verified, tested, and recoverable backups do.

SofTouchSystems.com
No-Surprise IT — Predictable. Proactive. Proven.