

Backup & Restore Checklist

What to protect and how to verify it before you need it.

Rule of thumb

Do not rely on a single backup copy stored on the same server as the live website.

What to Back Up

- Website and application files.
- Databases.
- Important mailbox data when required by your recovery plan.
- Configuration files, DNS notes and scheduled-task information.

How Often

- Use a schedule that matches how frequently the site changes.
- Take an extra backup before application or plugin updates.
- Take a backup before migrations or major configuration changes.
- Increase backup frequency for ecommerce, forums and other frequently changing systems.

Where to Store Backups

- Keep at least one copy outside the production server.
- Use access-controlled cloud or local storage.
- Keep multiple restore points so one bad backup does not replace every good copy.
- Restrict backup access because backups may contain sensitive data.

Verify the Backup

- Confirm the archive opens successfully.
- Check timestamps and file sizes for obvious failures.
- Verify database exports are non-empty and readable.
- Perform an occasional test restore into a safe location.

Restore Readiness

- Know which components must be restored first.
- Document the restore process and required credentials.
- Keep the original backup unchanged while testing a restoration.
- After restore, test website, database, email and scheduled tasks.

Backup Checklist

- | |
|--------------------------------|
| ✓ Files included |
| ✓ Database included |
| ✓ Off-server copy exists |
| ✓ Multiple restore points kept |
| ✓ Backup opens |
| ✓ Database export checked |
| ✓ Restore process documented |
| ✓ Test restore performed |