

Website Migration Policy

Compatibility, access and verification for an organized move.

Key points for reference

- One compatible initial website migration included.
- Scope and timing confirmed after technical review.
- Keep the source active until validating the move.

Reference summary. The complete clauses below prevail.

1. Benefit and scope

Initial hosting includes one compatible initial site migration to the purchased plan. This is transfer of the agreed scope, not redesign, unlimited updates, code repair or malware cleanup. Extra sites, accounts, external mailboxes or stages require assessment and an accepted quotation.

Moving files and databases does not transfer domain registration or ownership. Registrar transfer, DNS changes and email migration are separate actions that must be identified. Paid extras are not added without confirmation.

2. Compatibility review

Review covers the source, panel, technologies, versions, volume, licenses, destination capacity and dependencies. The plan must fit the content. Corruption, obsolete applications, missing keys or source-provider restrictions may prevent or change the process.

The response states scope, exclusions, adjustments, prerequisites, window and extra costs. Incompatibility is not resolved by deleting content or replacing applications without permission. Customers accept alternatives before cutover.

3. Authorization and credentials

Requesters must have authority over the account, website and data. Prefer temporary least-privilege access through the secure mechanism specified by authenticated support. Do not submit passwords or authentication codes through public forms.

Access is limited to the authorized work, not other accounts or permanent use. Revoke temporary access and rotate shared credentials afterward. Keep the source available while needed.

4. Initial copy and changing data

Keep an independent copy and identify the extraction time. Stores and continuously updated systems may receive later orders, messages or changes. Final synchronization, a write pause or another appropriate strategy must be agreed; one copy does not automatically include later changes.

Email needs its own scope: mailboxes, passwords, calendars and contacts do not necessarily transfer together. Payments, webhooks and integrations may require testing by the responsible party.

5. Validation before DNS changes

Where feasible, validate the destination before DNS changes. Check pages, images, databases, login, forms, scheduled tasks, certificates and critical integrations. A working homepage does not validate the whole system.

DNS changes must account for records, caching and TTL without an instant-propagation guarantee. Visitors may reach different environments during transition. Record authorized changes, cutover ownership and rollback.

6. Timing, communication and obstacles

Timing and the window are confirmed after review and receipt of required access. Payment does not automatically start a promised execution window. Volume, source bandwidth, export restrictions, availability and errors may change estimates.

Obstacles require explanation of cause, impact and next steps before scope or price increases. Delays are not automatically blamed on customers. Decisions, revised windows and protective pauses are recorded.

7. Completion, rollback and closing the source

Completion identifies transferred content, tests, specific outstanding items and changes. Validate before canceling the old provider or deleting your copy. Zovvi does not cancel that contract without specific authorization.

Rollback must account for new destination data and DNS changes and may require reconciliation, not just repointing. Revoke access and check backups, domains and integrations afterward. This policy does not reduce legal remedies for Zovvi execution failures.