

Website Ownership, Access & Handover Policy

A practical transparency guide explaining who owns each website asset, how Web Lab gets the access needed to work, and how control is preserved for the client. A signed proposal, statement of work, service agreement, or platform-specific limitation may define additional or different terms for a particular project. Where there is a conflict, the signed project agreement should be followed.

1. Ownership & Access at a Glance

The preferred setup is client ownership with delegated Web Lab access. The client retains control of critical business assets, while Web Lab receives the minimum practical permissions needed to perform the agreed work. Where the client does not have a required technical service or prefers a hands-off arrangement, Web Lab can provide or manage that service under an agreed scope and cost, with ownership and handover kept transparent.

Core principle — *Your business assets remain yours. Web Lab by Ashik receives only the access reasonably needed to design, build, launch, maintain, and support the website. The service should never depend on the client being locked out of critical accounts.*

Asset / Service	Preferred Owner	Web Lab Access
Domain registration	Client	Delegated/admin access when needed
DNS	Client or client-designated provider	Technical access to configure records
Website hosting	Preferably client; managed option possible	Admin/developer access
Source code	As defined in project agreement; normally client project code after payment	Developer access while engaged
CMS / website admin	Client	Admin/editor access
Email mailbox	Client	No mailbox access unless specifically required and approved
Forms / transactional email	Client account where practical	Configuration access
Analytics / Search Console	Client	Administrator or editor access
Third-party tools	Client where practical	Role-based access
Backups	Client project data remains client asset	Access needed to create/restore
Content & media	Client-owned or properly licensed	Access to use for project

Recommended model — *Where a platform supports collaborators, users, teams, or delegated roles, the client should invite Web Lab instead of sharing the primary account password.*

2. Web Lab-Managed Services & Assisted Setup

The client is not required to personally create, configure, or manage every technical service described in this policy. If the client does not already have a required account, service, infrastructure component, or technical setup—or simply prefers not to manage it—Web Lab by Ashik can assist with selecting, creating, configuring, operating, and maintaining an appropriate solution where technically and commercially practical.

This may include, where relevant:

- Domain registrar and DNS setup or management.
- Website hosting, deployment, CDN, storage, and related infrastructure.
- Source-code repository / version-control setup when the client does not already have one.
- CMS administration and website-management accounts.
- Contact-form delivery, transactional email, notifications, and related lead-delivery services.
- Analytics, Search Console, monitoring, backups, and performance tools.
- Third-party integrations, plugins, APIs, and other services required to operate the website.
- Ongoing technical maintenance, troubleshooting, and support.
- Content or creative services such as substantial copywriting, logo/brand design, custom graphics, photo editing, or other new design work when separately requested.

Cost & approval rule

- Before Web Lab enables a paid third-party service, purchases a subscription, introduces a recurring cost, or begins work outside the agreed project or maintenance scope, the expected cost and responsibility for payment will be explained to the client and agreed in advance.
- No additional management fee, setup fee, subscription charge, creative-service fee, or other out-of-scope cost should be incurred on the client's behalf without prior agreement.
- Where possible, third-party services should be placed directly in the client's account so the client can see billing, ownership, and renewal information. If a Web Lab-managed service is more practical, that arrangement and any related fee should be documented clearly.
- The client may choose to manage a service directly, ask Web Lab to manage it, or use a shared/delegated-access model, depending on the platform and the agreed service scope.

Ownership & handover rule

- Web Lab-managed support should not unnecessarily remove the client's ownership, access, recovery rights, or ability to change providers later.
- Where Web Lab creates or manages an account on the client's behalf, the preferred setup is to document the account, billing model, access method, and handover path.
- If the relationship ends, services and assets should be handed over according to the applicable project or maintenance agreement, subject to payment of any outstanding agreed charges.

General service principle — *If the client does not have a required service or prefers not to manage it, Web Lab by Ashik can usually assist or manage it under an agreed arrangement. Any additional work, recurring service, third-party cost, or management fee is explained and agreed beforehand, while preserving appropriate client ownership, access, and a clear handover path.*

3. Domain Ownership

The domain name should remain registered in the client's name or business account whenever possible. Web Lab by Ashik does not need to own the client's domain in order to build, launch, or maintain the website.

How Web Lab works with the domain

- Web Lab may need access to the registrar or DNS settings to connect the domain, configure SSL, verify services, migrate hosting, or troubleshoot domain-related issues.
- Where delegated access or additional-user roles are available, the client should grant Web Lab the minimum permission required.
- If delegated access is unavailable, the client may make requested changes themselves using instructions from Web Lab, or provide temporary access if both parties agree.

What remains under client control

- Registrar account and domain ownership information.
- Renewal settings and billing.
- Recovery email, recovery phone, and multi-factor authentication.
- Transfer authorization / EPP controls.

Web Lab should not transfer the domain, change legal ownership, disable renewal, or make ownership-level changes without the client's approval.

Principle — *The client owns the domain. Web Lab receives only the access needed to manage its technical configuration.*

4. DNS Management

DNS connects the domain to the website, email, analytics verification, and other services. Because a DNS mistake can affect both the website and business email, changes should be controlled and documented.

How Web Lab accesses DNS

- Prefer delegated DNS access through Cloudflare, the registrar, or another DNS provider.
- Web Lab may add or update records such as A, AAAA, CNAME, TXT, SPF, DKIM, DMARC, and verification records when required by the project.
- Existing records should be reviewed before changes are made, especially MX/email records.

Approval boundary

- Routine website connection records may be changed as part of approved launch/maintenance work.
- Changes that may interrupt email, transfer DNS providers, or materially change infrastructure should be discussed with the client first.
- Web Lab should keep a simple record of important DNS changes so they can be reversed or handed over.

Principle — *DNS may be technically managed by Web Lab, but the client should retain administrative control of the DNS account or provider relationship.*

5. Hosting & Infrastructure

Hosting is where the website runs. Two models are supported: client-owned infrastructure and Web Lab-managed infrastructure.

Option A — Client-owned hosting (preferred where practical)

- The client creates or owns the hosting account.
- The client invites Web Lab as an administrator, developer, collaborator, or team member.
- Web Lab deploys, configures, monitors, and maintains the website using that delegated access.
- Billing and account recovery remain directly under client control.

Option B — Web Lab-managed hosting

- Web Lab may host the site within infrastructure it manages when this is simpler or part of a care plan.
- The proposal should make the managed-hosting arrangement clear, including any recurring fee.
- The client still owns its business content and project data.
- If the relationship ends, Web Lab should provide a reasonable export/handover path for the website so it can be moved to another compatible host.

Access while working

- Web Lab may require deployment, server, database, CDN, storage, or environment-configuration access depending on the architecture.
- Access should be limited to the services required for the website.
- Production changes should be made carefully and, where practical, through version-controlled deployment rather than ad-hoc edits.

Principle — *The hosting model should be known in advance. Client-owned accounts maximize independence; managed hosting maximizes convenience but must still support a clear handover path.*

6. Source Code & Repository

Source code should be stored in a version-control system (VCS) such as GitHub, GitLab, Bitbucket, or another agreed platform. Ownership, access, and handover rights should be stated clearly in the project agreement.

Recommended arrangement

- If the client already has a suitable version-control system or repository, the preferred approach is for the client to own that repository and invite Web Lab as a collaborator with the access.
- If the client does not have a VCS/repository, Web Lab may create and use a repository under Web Lab's own version-control account during development and maintenance.
- When Web Lab uses its own repository, the client-specific source code will be handed over or transferred to the client after the agreed project payment has been completed, if the client requests it.
- The handover may be provided by transferring the repository to a client-owned VCS account, granting repository access, or providing an agreed source-code export, depending on the platform and project arrangement.
- Reusable Web Lab components, internal tools, frameworks, libraries, build systems, or licensed third-party code remain subject to their existing ownership and license terms and are not automatically transferred as exclusive client property.

How Web Lab works with the code

- Web Lab requires repository write/deploy access while actively developing or maintaining the website. Where the repository is client-owned, this should normally be provided through a separate collaborator account.
- Changes should be committed to version control so there is a traceable development and maintenance history.
- Production secrets, credentials, and private environment values should not be committed to the repository.

Principle — *The client should have a clear path to obtain the client-specific source code. If Web Lab hosts the repository because the client does not have a VCS, the code can be handed over after project payment when requested.*

7. CMS & Website Administration

If the website uses a CMS or site-management dashboard, the client should retain a primary administrator account.

- Web Lab should receive a separate named administrator/editor account rather than using the client's personal login.
- Permissions should match the work required: content editing, plugin/theme maintenance, settings, or full administration.
- Web Lab may create staging or test environments where the platform supports them.
- Critical changes should be tested before production where practical.
- If Web Lab's engagement ends, its user account can be removed without affecting the client's ownership or access.

Principle — *Separate user accounts create accountability and make access easy to grant, audit, or revoke.*

8. Business Email, Contact Forms & Lead Delivery

Business email accounts remain client assets. Web Lab normally does not need access to the client's mailbox in order to make website forms work.

How Web Lab supports forms

- Configure contact, quote, booking-interest, or project-inquiry forms as agreed.
- Connect form delivery to the client's designated business email or approved CRM/tool.
- Configure transactional-email services where required.
- Test form validation and delivery during launch and maintenance.
- Monitor or periodically check important forms when included in the maintenance plan.

Form delivery services & costs

- Some website forms require a third-party transactional email, SMTP, form-processing, CRM, or notification service to reliably deliver messages to the client. Examples may include services such as Resend, Postmark, Mailgun, SendGrid, Formspree, or an equivalent provider.
- Where practical, the preferred setup is for the client to own the relevant third-party account and invite Web Lab with the access needed to configure and maintain it.

- If Web Lab provides or manages the delivery service through its own account as part of a hosting or care arrangement, that dependency and any included limits should be made clear to the client.
- Free tiers may be suitable for low-volume websites, but they are controlled by the third-party provider and may change, expire, impose limits, or become insufficient as usage grows.
- Any recurring third-party fee for form delivery, transactional email, SMS, CRM, or similar services is normally a client cost unless the signed project or maintenance plan explicitly states that it is included.
- If a new paid service becomes necessary, Web Lab should explain the reason and expected cost and obtain the client's agreement before enabling a new recurring charge.
- Web Lab can configure, test, monitor, and troubleshoot the technical delivery path, but availability and pricing of external providers remain subject to those providers' own services and terms.

Email access

- Web Lab should not request full mailbox access merely to configure a form.
- If mailbox-level access becomes genuinely necessary for troubleshooting, it should be time-limited and explicitly approved.
- DNS records for email (MX, SPF, DKIM, DMARC) should be handled carefully because errors can interrupt business communication.

Principle — *The goal is reliable lead delivery without making Web Lab the owner of the client's email account.*

9. Analytics, Search Console & Marketing Integrations

Analytics and search data can become valuable business history over time, so these accounts should generally belong to the client.

- Google Analytics, Search Console, Tag Manager, advertising accounts, and similar platforms should preferably be created in the client's account.
- Web Lab may receive administrator/editor access to configure tracking, troubleshoot issues, or review performance.
- If Web Lab creates an account temporarily during setup, ownership/access should be transferred or shared with the client promptly.

- Tracking should not intentionally collect sensitive form contents or unnecessary personal information.

Principle — *Historical analytics and marketing data should stay with the business even if the service provider changes.*

10. Third-Party Services, Licenses & Subscriptions

Websites may depend on third-party services such as forms, email delivery, maps, scheduling, fonts, image libraries, plugins, APIs, CDN services, or paid integrations.

- Client-owned accounts are preferred when the service is business-critical or has recurring billing.
- If a Web Lab-managed license is used, the proposal should identify whether continued use depends on an active Web Lab service plan.
- Third-party pricing and terms can change independently of Web Lab.
- Web Lab should document important dependencies so the client understands what the website relies on.

Principle — *A client should know which parts of the website depend on external vendors and who pays for each one.*

11. Credentials, Security & Access Control

Access should be granted in a way that minimizes unnecessary exposure of passwords and reduces the risk of account lockout.

Preferred access method

- Use collaborator/team/admin invitations instead of shared master passwords whenever supported.
- Use separate Web Lab user accounts so access can be revoked independently.
- Enable multi-factor authentication on critical registrar, hosting, email, and source-control accounts.
- Use password managers or secure one-time sharing methods if a password must be shared.
- Avoid sending passwords in ordinary email or chat where a safer method is available.

Access lifecycle

- Grant only the permission required for the task.
- Increase access temporarily when a specific task requires it.
- Reduce or remove access when the task or service relationship ends.
- Web Lab should not change recovery details or account ownership unless explicitly required and approved.

Principle — *The client remains the recovery authority for critical business accounts.*

12. Backups, Recovery & Website Continuity

Backups are part of reducing operational risk, but the exact backup model depends on the platform and maintenance plan.

- Where supported, Web Lab can configure automated website/database backups.
- Backups may be stored by the hosting provider, a separate storage provider, or both.
- Retention periods and restore points should match the importance and update frequency of the site.
- Web Lab may need hosting/database access to create or restore backups.
- A restore should be tested or verified when practical, especially for business-critical sites.
- Client project data remains the client's asset even when a backup is stored in Web Lab-managed infrastructure.

Principle — *A backup is useful only if it can be restored. Critical sites should have a documented recovery path.*

13. Maintenance, Monitoring & Updates

Maintenance is intended to keep the website technically healthy and reduce the chance that important issues remain unnoticed for long periods.

Typical maintenance access

- Web Lab may retain delegated access to hosting, CMS, source code, forms, analytics, DNS, or monitoring tools for the duration of the maintenance service.
- Access is used only for agreed website-management purposes.

Typical essential maintenance

- Technical dependency/software updates where applicable.
- Basic availability/uptime checks.
- Contact and lead-form checks.
- Small technical fixes and troubleshooting.
- Hosting/deployment assistance.
- Performance checks.
- Backup oversight where included.
- Support when the website has a technical issue.

Normally outside essential maintenance

- Major redesigns.
- Unlimited content changes.
- New pages beyond the agreed scope.
- New features or integrations.
- Large content migrations.
- Custom application development.

Additional work can be quoted separately before it begins.

Principle — *Maintenance means responsible technical care, not unlimited future development.*

14. Content, Images, Brand Assets & Intellectual Property

The client should provide or approve business content, logos, photographs, videos, service information, reviews, and other brand assets used on the production website.

- Client-supplied assets remain the client's property or subject to the client's existing rights.
- Web Lab may use properly licensed stock photography, icons, fonts, or other third-party assets where appropriate.
- Third-party licenses remain subject to their original terms.
- Web Lab should not claim ownership over the client's business name, logo, customer data, or original business photography.
- Portfolio/display rights, if any, should follow the project agreement or client permission.

Additional content and design work

- Essential maintenance or free post-launch support does not automatically include creation of new marketing content or new creative/design assets.
- Work such as copywriting, writing substantial new page content, logo design, brand identity work, custom illustrations, social graphics, brochures, extensive photo editing, video production, or other new creative assets is outside essential maintenance unless it was explicitly included in the original project scope.
- If the client requests this type of content or design work after launch, Web Lab will first clarify the requirement and agree any additional cost before the work begins.
- Minor placement or replacement of client-supplied and already-approved text, images, logos, or contact information may still be handled as part of maintenance when the applicable care plan includes small content updates.
- Where Web Lab arranges third-party photography, stock assets, fonts, copywriting, design services, or other licensed creative resources, any applicable third-party costs should also be disclosed and agreed before purchase.

Principle — *Client brand assets remain client assets; third-party materials remain subject to their licenses.*

15. Billing, Renewals & Recurring Costs

A client should know which costs belong to the website project, which are optional additional services, and which are third-party recurring expenses.

- Domain renewal, hosting, business email, paid plugins, transactional email, scheduling, or other vendor fees should be identified where relevant.
- Where possible, recurring vendor charges should be billed directly to the client's account.
- If Web Lab bundles a recurring service into a maintenance/care plan, the included services should be stated clearly.
- Web Lab should not intentionally make a client dependent on hidden third-party charges.

Principle — *Project fees and recurring platform/vendor costs should be transparent and distinguishable.*

16. Client Data & Privacy

Forms, analytics, customer inquiries, and website databases may contain personal or business information. Access should be limited to what is required to provide the service.

- Web Lab should avoid collecting or retaining unnecessary personal data.
- Production credentials and customer data should not be copied into development environments unless reasonably required and appropriately protected.
- Form submissions should be sent only to approved destinations.
- If a third-party processor is used, the client should be informed where practical.
- When the engagement ends, Web Lab should remove unnecessary retained access and data copies, subject to legal, billing, backup, or support requirements.

Principle — *Access to client data is for service delivery, not ownership or unrelated use.*

17. Changes That Require Client Approval

Web Lab can perform routine technical work under the agreed scope, but ownership-level or materially disruptive changes should not happen silently.

- Transferring the domain to another registrar.
- Changing domain ownership or recovery information.
- Moving DNS to a different provider when it could affect email or other services.
- Changing business email providers or MX records.
- Deleting major production data.
- Changing hosting architecture in a way that creates new recurring costs.
- Purchasing paid third-party services not already approved.
- Publishing substantial new business claims/content not provided or approved by the client.
- Launching a major redesign when the project requires explicit approval.

Principle — *Routine maintenance can be delegated. Material ownership, billing, or business-impacting decisions remain with the client.*

18. Handover & End of Service

If the client chooses to move to another provider or end maintenance, Web Lab should support an orderly handover rather than create unnecessary technical dependency.

Typical handover items

- Current source-code repository or agreed code delivery.
- Hosting/deployment information.
- DNS configuration summary.
- CMS/admin access information.
- Important third-party service list.
- Analytics/Search Console access.
- Relevant backup/export files where applicable.
- Known technical notes or outstanding issues.

Access removal

- After handover, the client may revoke Web Lab's accounts/roles.
- Web Lab should remove unnecessary stored credentials and local copies when no longer required.
- If a service is hosted inside Web Lab-managed infrastructure, reasonable migration/export assistance should be provided according to the service agreement.

Principle — *The client should be able to continue operating the website without Web Lab being the only person who knows how to access it.*

19. If Web Lab Becomes Unavailable

A transparent setup should reduce dependence on any single person. The recommended ownership model is designed so the client can recover and continue operating critical services even if Web Lab is temporarily or permanently unavailable.

- Client retains registrar/recovery control.
- Client has access to hosting or a documented managed-hosting handover path.
- Client has repository/code access according to the project agreement.
- Client retains analytics, email, and other core business accounts.
- Critical third-party dependencies are documented.
- Backups and recovery paths are defined where included.

Principle — *Reliability comes from reducing single-person dependency, not from asking the client to trust one provider blindly.*

20. Client Responsibilities

Transparency works best when both parties keep access and business information current.

- Maintain current billing for domains, hosting, email, and required third-party services.
- Keep account recovery information and multi-factor authentication accessible.
- Provide accurate business information and approved content.
- Notify Web Lab before making major DNS, hosting, or account changes that could affect the website.
- Keep a current internal record of who has administrative access to critical business accounts.
- Inform Web Lab promptly when business contact details, services, locations, or ownership information change.

21. Practical Access Matrix

The table below summarizes the preferred operational model during an active Web Lab engagement.

System	Client Access	Web Lab Access	Who Approves Changes?
Domain registrar	Client master/admin	Delegated admin or temporary technical access	Client approval for transfer/ownership changes
DNS	Client/provider admin	DNS editor/admin	Web Lab for routine website records; client for disruptive changes
Hosting	Client preferred; Web Lab-managed optional	Developer/admin	As defined by hosting model
Source repository	Client preferred / agreed ownership	Write/deploy access	Web Lab during development; client retains project access
CMS	Client admin	Separate Web Lab admin/editor	Web Lab within scope
Email mailbox	Client	Normally none	Client
Email/DNS configuration	Client	Technical configuration access	Web Lab within approved setup
Forms	Client business process	Admin/configuration access	Web Lab for technical configuration
Analytics/Search Console	Client	Admin/editor	Web Lab for setup/maintenance
Third-party tools	Client where practical	Role-based access	Depends on tool and scope
Backups	Client data ownership	Backup/restore access	Web Lab when included

22. Closing Commitment

Web Lab by Ashik's goal is to make website ownership easier, not more dependent. The client should understand what exists, who owns it, where it is hosted, how Web Lab accesses it, what is being maintained, and how control can be handed back at any time.

Web Lab commitment — Build and support the website with enough access to do the job properly, while preserving the client's ownership, recovery options, and long-term independence.