



MageLabs Inc.

Saito Building III, 5F 34,
Udagawacho 34-5, Shibuya
Tokyo 150-0042, Japan

Client Intellectual Property and Data Protection Protocol

Version 1.0 (2026-03-17)

1. Intellectual Property (IP) Rights & Ownership

To accelerate development and improve quality, MageLabs may utilize certain pre-existing "Foundational IP" during an engagement. This refers strictly to internal frameworks, utility libraries, and scaffolding developed independently by MageLabs.

1.1. Perpetual License for Foundational IP

Where this Foundational IP is integrated into the final deliverables, the client is automatically granted a perpetual, royalty-free, non-exclusive license to use, modify, and maintain that foundational code within the delivered product, as well as in any future products or derivative works developed by the client.

1.2. Client Ownership of Deliverables & Domain Logic

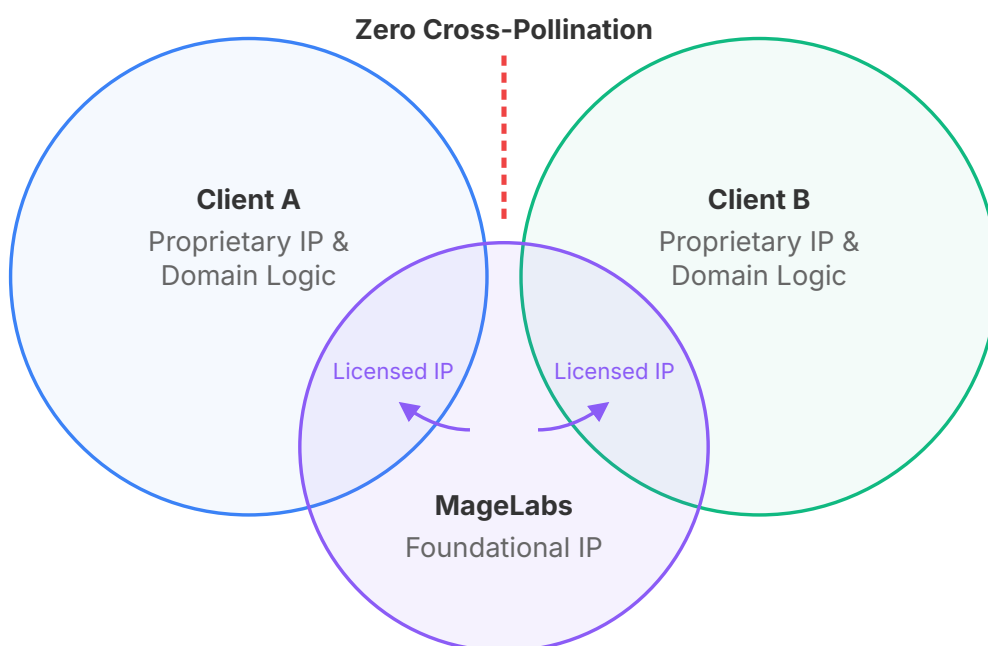
The client owns all exclusive IP rights to the deliverables formally scoped and funded under the engagement. MageLabs retains no rights over the client's proprietary source code and domain logic. However, MageLabs retains ownership of the Foundational IP developed independently of the client's core business logic.

1.3. No Restrictive Licenses

MageLabs will never introduce restrictive or "copyleft" open-source components (such as GPL-licensed code) into the client's proprietary deliverables without the client's explicit prior written consent.

1.4. Strict Reuse Boundaries

MageLabs never reuses code between client projects. The only exceptions are our pre-existing Foundational IP and insignificant, general-purpose implementation details that contain no domain-specific or application-specific logic.



2. Infrastructure & Operational Security

2.1. Infrastructure Segregation

All client code, data, and documentation reside in strictly isolated environments. Depending on the engagement, we utilize:

- Client-provisioned infrastructure.
- Single-tenant cloud environments, configured exclusively for the client's project.
- Secure local workstations, with full-disk encryption and strict access control.

We prohibit the use of shared hosting or multi-tenant development servers.

2.2. Access Control & Endpoint Security

Access is granted strictly on a principle of least privilege. All MageLabs engineering workstations are protected by full-disk encryption, and strictly controlled local storage policies. Client data is never synchronized to personal devices.

2.3. Post-Engagement Erasure

Upon contract termination or project delivery, all proprietary data, code repositories, and development environments hosted by MageLabs are subject to secure cryptographic erasure, accompanied by a formal confirmation of deletion.

