MarocAgency — Data Retention & Records Management Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: CEO / Compliance Manager

1. Purpose

This policy defines how MarocAgency retains, archives, and disposes of all records and data produced or handled by the company — including client data, project deliverables, internal documents, logs, backups — to ensure regulatory compliance, data lifecycle management, and secure disposal when data is no longer needed.

2. Scope

Applies to all data stored, processed or managed by MarocAgency, whether digital or physical. This includes, but is not limited to:

- Client data (e.g. leads, contact lists, marketing data)
- Project data (websites, code repositories, deliverables)
- Internal corporate documents (contracts, HR records, financial records)
- System data (logs, access logs, audit logs)
- Backups, archives, email correspondence, shared documents
- Data held by third-party vendors or subcontractors working on behalf of MarocAgency

3. Definitions

- **Record** — any file, document, database entry, log, email, backup, or other piece of information created or managed by MarocAgency.
- **Retention Period** — the minimum period data must be kept before being eligible for archiving or secure deletion.
- **Archive** — secure, long-term storage for records that are inactive but may need future retrieval.
- **Deletion / Destruction** — secure erasure of digital records or secure destruction of physical records once retention period ends or when appropriate.
- **Legal / Contractual Hold** — suspension of any archiving or deletion when data is required to be kept due to contract, audit, litigation, or regulatory obligations.

4. Retention Schedule

Data / Record Type	Retention Period
Active client data (leads, contact lists)	Duration of the client contract + 3 years
Client data after contract termination (unless requested deletion)	3 years post-termination
Project deliverables & source code repositories	Indefinite (archived backup); inactive branches or deprecated projects archived after 2 years
Financial & accounting records (invoices, payments, tax)	7 years
Employee / HR records (contracts, payroll, evaluations)	10 years after end of employment
System logs (access logs, error logs, audit logs)	18 months (archive at 6 months, then purge)
Backups (weekly snapshots)	90 days
Monthly full backups / archived backups	2 years
Internal communications (emails, memos)	2 years unless flagged for long-term retention
Vendor/subcontractor contracts & records	5 years after contract end

5. Archiving & Deletion Procedures

- Archived data must be encrypted at rest and in transit if stored off-site or in cloud.
- Archived data must be stored with access controls; only authorized roles may retrieve.
- After retention period expires (and no Legal / Contractual Hold), records must be securely deleted (digital) or securely destroyed (physical).
- All archive or deletion operations must be logged: actor, date/time, data type, reason.
- Quarterly review of data eligible for archival or deletion.

6. Legal / Contractual Holds & Exceptions

- If a contract, audit, client request, litigation or regulatory obligation requires data to be retained beyond standard retention period, a Legal Hold must be placed.
- Data under Legal Hold cannot be archived or deleted until explicit release.
- Legal / Compliance Manager must authorize any exception or hold.

7. Roles & Responsibilities

- **Data Owner** (e.g. Project Manager, Department Head): classify data type, request retention/archiving/deletion when applicable.

- **IT / DevOps Team**: implement storage, backups, archiving, secure deletion; enforce encryption and access controls.
- **Compliance / Legal Manager**: monitor policy compliance, manage legal holds, handle audits and retention schedule reviews.
- **All Employees / Contractors / Vendors**: comply with this policy; do not bypass archiving or deletion procedures; report any irregularities.

8. Policy Review & Revision

- The policy must be reviewed at least once per year, or when relevant laws/regulations change, or when MarocAgency's services change.
- Maintain version history (version number, date, approver, change summary).
- Communicate any updates to all staff and require acknowledgment.