MarocAgency — Data Classification & Confidentiality Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: Security & Compliance Manager

1. Purpose

This policy defines classification levels for all data managed by MarocAgency, establishes handling rules based on classification, and ensures confidentiality, integrity, and proper protection of internal and client data.

2. Scope

Applies to all data processed, stored, or handled by MarocAgency — including client data, lead data, marketing data, project files (code, documents), internal documents (contracts, HR, financial), backups, logs, communications, vendor/subcontractor data — regardless of format (digital, paper, cloud).

3. Classification Levels

Classification Level	Description
Public	Data intended for public use or release (e.g. public website content, blog posts, marketing brochures).
Internal	Internal documents not containing sensitive info (e.g. internal memos, general admin documents, meeting notes).
Confidential	Sensitive business or client data: project source code, lead databases, client contact data, vendor contracts, internal financial or strategic documents.
Highly Confidential / Personal Data	Client personal identifiable information (PII), employee personal data, authentication credentials, encryption keys, payment data, security logs, backups containing sensitive data.

4. Access Control & Handling Rules

- Access to data must follow **Role-Based Access Control (RBAC)** and **least-privilege principle**.

- Confidential and Highly Confidential data must be encrypted at rest and in transit (e.g., TLS for transfers, disk or storage encryption).
- Any sharing with external parties (clients, vendors, subcontractors) requires a valid Data-Processing / Data-Sharing Agreement (DPA), and secure, encrypted transfer.
- Internal sharing of sensitive data must use secure channels: company VPN, encrypted file sharing, authenticated access.

5. Employee / Contractor / Vendor Obligations

- All employees, contractors, and vendors must sign a confidentiality / non-disclosure agreement (NDA) on onboarding.
- No unauthorized personal use of company or client data; no storage on personal devices unless explicitly approved and encrypted.
- On termination (resignation, contract end): revoke access, collect credentials/devices, ensure deletion or return of all sensitive data, archive or transfer project data per Data Retention Policy.

6. Data Breach & Incident Reporting

- Any suspected or confirmed unauthorized access, leak, or data breach must be reported **within 24 hours** to Security & Compliance Manager.
- Immediately trigger Incident Response & Data Breach Policy workflow.
- Notify affected clients or data subjects if personal data is involved — in accordance with contractual obligations and applicable data protection laws.

7. Audit & Compliance Monitoring

- Quarterly audit of access logs to Confidential / Highly Confidential data.
- Bi-annual review of user access rights and permissions.
- Verification of encryption, secure storage, and correct handling procedures.
- Document and approve any exception or deviation from policy.

8. Policy Review & Update

- Annual review or sooner if business operations, services, or regulatory requirements change.
- Maintain version history (version number, date, author, approver, change log).
- Communicate updates to all staff and require acknowledgment.