MarocAgency — Software Development & Secure Coding Guidelines

Version: 1.0

Effective Date: 2025-12-03

Approved by: CTO / Head of Engineering

1. Purpose

Ensure that software and web solutions developed by MarocAgency meet high standards of security, quality, confidentiality, and compliance — protecting client data, maintaining integrity, and reducing vulnerabilities.

2. Scope

All development projects, code repositories, scripts, services, applications, automation tools, websites, and infrastructure managed by MarocAgency — including internal tools, client projects, APIs, databases, and deployment pipelines.

3. Secure Coding Practices & Standards

- Input validation and sanitization to prevent injection attacks.
- Use of parameterized queries or ORM for database access.
- Proper error handling without leaking sensitive information.
- Encryption of sensitive data (in transit and at rest) — especially client data, credentials, payment info, PII.
- Avoid hardcoding secrets (credentials, API keys); use secure secret management.
- Principle of least privilege: services and modules access only what is necessary.

4. Code Review & Version Control

- All code changes merging to main / master / production branches must undergo peer code review.
- Review must include security assessment, code quality, compliance with standards.
- Maintain detailed commit history, use signed commits for critical codebases.

5. Dependency & Vulnerability Management

- Regular updates of dependencies and libraries.
- Perform vulnerability scans (static and dynamic) before each release.
- Track third-party licenses, and ensure no license violations.
- Remove unused dependencies and audit their risk.

6. Logging, Monitoring & Error Handling

- Log security-relevant events: authentication, data access, admin actions, permission changes.
- Logs must not contain sensitive data (passwords, keys, PII).
- Follow backup and retention policy for logs.

7. Deployment & Environment Separation

- Maintain separate environments: development, staging, production.
- Client data must never be used in non-production environments unless anonymized or pseudonymized.
- Configuration management via environment variables or secure secret management.

8. Training & Awareness

- All developers must undergo secure coding and data protection training at onboarding and annually.
- Document coding standards; make them accessible to entire engineering team.

9. Roles & Responsibilities

- **Developers / Engineers:** comply with coding standards, follow review and deployment procedures.
- **Tech Leads / Reviewers:** perform code reviews, enforce policies, approve merges.
- **DevOps / IT Team:** manage deployment environments, secret management, environment separation, backups.
- **Security / Compliance Team:** audit practices, report vulnerabilities, enforce remediation.

10. Policy Review & Update

- Review guidelines annually or when security threats evolve.
- Update coding standards and security practices accordingly.
- Communicate changes to the development team and require compliance.