MarocAgency — Change Management & Deployment Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: CTO / IT Director

1. Purpose

Establish controlled processes for all changes to infrastructure, systems, applications, and deployments — ensuring stability, traceability, security, and preventing unplanned disruptions or data exposure.

2. Scope

All system infrastructure, servers, databases, production environments, cloud services, deployment pipelines, configuration changes, access changes, and any software or service update managed by MarocAgency.

3. Change Request Process

- Any proposed change must be submitted via a Change Request Form with: description, rationale, affected systems, rollback plan, risk assessment.
- Change Manager reviews the request; high-risk changes require additional approval (CTO / Security Manager).
- Schedule the change (maintenance window), notify affected teams/clients in advance.

4. Deployment & Change Execution

- Changes must first be tested in staging or development environments.
- After testing, deploy to production with minimal downtime and rollback plan.
- Record deployment/change logs: who performed, when, what changed, justification, results.

5. Emergency / Hotfix Changes

- Emergency fixes allowed only for critical failures/security issues.
- Must be documented after the fact, with justification and approval.

- Post-deployment review mandatory; rollback if issues arise.

6. Access & Configuration Changes

- Changes to permissions, access rights, configurations must follow access control policy.
- Document all modifications; maintain versioned configuration history.

7. Audit & Review of Changes

- Monthly review of change logs.
- Quarterly evaluation of change management effectiveness: downtime events, incidents related to change, rollback frequency.
- Update procedures and improve risk assessment based on review findings.

8. Roles & Responsibilities

- **Change Manager / IT Lead:** triage change requests, approve changes, manage deployment schedule.
- **Developers / DevOps Engineers:** implement changes, test, deploy, log operations, restore if needed.
- **Project / Data Owners:** assess impact on clients or data, request change if needed.
- **Security / Compliance Manager:** review risky changes, ensure compliance and security standards.

9. Policy Review & Maintenance

- Review of this policy at least every 6 months or after major incidents.
- Maintain versioning, documentation of changes, and communicate updates.