MarocAgency — Internal Audit & Compliance Procedure

Version: 1.0

Effective Date: 2025-12-03

Approved by: Compliance & Security Manager

1. Purpose

Ensure that MarocAgency operates in accordance with its internal policies (data retention, confidentiality, access control, backups, change management, etc.), regulatory requirements, and best practices — by periodically reviewing, auditing, and enforcing compliance.

2. Scope

All departments, data stores, systems, logs, backups, project data, employee data, access rights, vendor access, and processes defined in company policies.

3. Audit Types & Frequency

- **Quarterly Audits:** Check compliance with data retention, access control, backup logs, user permissions, change logs.
- **Ad-hoc Audits:** Triggered after security incidents, data breach, or upon request from management or clients.
- **Annual Comprehensive Audit:** Full review of all policies, procedures, data flows, logs, compliance with confidentiality and retention requirements.

4. Audit Process

1. Define audit scope and objectives.
2. Collect data: logs, records, backups, user permissions, project data, vendor contracts.
3. Compare against policy requirements.
4. Document findings: compliance issues, policy violations, risks, observations.
5. Issue audit report with recommendations.
6. Assign remediation tasks, track progress, follow-up.

5. Non-Compliance & Remediation

- For any detected non-compliance, create a remediation plan with deadline.
- Responsible managers must implement corrective measures.
- Repeat audit to confirm compliance.
- Persistent non-compliance escalated to senior management.

6. Documentation & Record Keeping

- Audit reports stored securely, retained per Data Retention Policy.
- Maintain history of audits, findings, remediation actions, and closures.

7. Roles & Responsibilities

- **Internal Audit Team / Compliance Officer:** plan and execute audits, compile reports, monitor remediation.
- **Department Heads / Data Owners:** cooperate with audits, respond to findings, implement corrections.
- **Security / IT Team:** provide access to logs, systems, data; assist in audit data collection.

8. Review & Update**

- Review audit procedure annually or after major changes.
- Update audit protocols to reflect any new policies or regulatory requirements.