MarocAgency — Incident Response & Data Breach Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: Security & Compliance Manager

1. Purpose

Define procedures and responsibilities for detecting, reporting, responding to, and recovering from security incidents or data breaches affecting MarocAgency's systems or data — thereby minimizing risk to clients, users, and the company.

2. Scope

Covers any security event, unauthorized access, data leak, system compromise, data loss, loss of integrity or confidentiality, or breach affecting client data, internal data, backups, logs, or infrastructure — whether caused internally or externally.

3. Incident Severity Classification

Severity Level	Description
Low	Minor incident, no sensitive data exposed, no service interruption, minimal impact.
Medium	Limited data or system impact, non-critical data involved, manageable recovery.
High	Sensitive data or client data involved, potential impact on clients or business operations.
Critical	Large-scale breach, significant data exposure, regulatory or contractual obligations triggered.

4. Incident Reporting & Notification

- Any employee who detects or suspects an incident must report it **within 24 hours** to Security & Compliance Manager.
- Security Manager logs the incident with date, time, reporter, and description of the event.

- For High or Critical incidents involving personal or client data: notify affected clients/data subjects and relevant authorities as required by law or contract, within contractual/regulatory deadlines.

5. Incident Response Process

1. **Detection & Verification** — confirm validity of the incident.
2. **Containment** — isolate affected systems/data to prevent further damage.
3. **Eradication & Recovery** — remove threat, patch systems, restore data from backups.
4. **Impact Assessment** — evaluate scope, data affected, affected clients or users, potential damage.
5. **Notification & Remediation** — communicate with stakeholders, implement mitigation measures, update policies or security posture as needed.
6. **Post-Mortem & Lessons Learned** — document cause, effect, actions taken, and propose improvements to prevent recurrence.

6. Logging & Evidence Preservation

- Preserve access logs, system snapshots, backup copies, relevant audit logs, and other evidence until investigation completes.
- Store evidence securely with restricted access, per confidentiality and retention policies.
- Maintain a full incident report file (timeline, actions, communications, remediation).

7. Roles & Responsibilities

- **All Staff**: report incidents promptly.
- **Security / IT Team**: lead response, containment, recovery, and remediation.
- **Compliance / Legal Team**: handle notifications, regulatory compliance, client communication.
- **Management / Executive Team**: oversee response, approve remediation plan, ensure resources, and implement improvements.

8. Training & Awareness

- Conduct security training upon onboarding for all employees/contractors/vendors.
- Perform at least one simulated incident drill per year (e.g. phishing simulation, breach recovery dry run).
- Review and update response procedures after drills or real incidents.

9. Policy Review & Maintenance

- Review this policy after each major incident; full review annually.
- Maintain version history, change log, and communicate updates to all stakeholders.