MarocAgency — Backup & Archiving Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: IT / DevOps Manager

1. Purpose

Ensure data integrity, availability, and recoverability by defining backup, archiving, and long-term storage procedures for all critical data assets managed by MarocAgency.

2. Scope

Covers all data and systems: databases, project repositories (code, assets), configuration files, client data, internal documents, logs, email archives, backups, cloud storage — whether local, on-premises, or in cloud.

3. Backup Strategy & Retention

Backup/Archive Type	Frequency / Retention
Daily incremental backups	Retained 30 days
Weekly full backups	Retained 90 days
Monthly full backups (archived)	Retained 2 years
Long-term archives (project deliverables, critical logs, compliance data)	Retained per Data Retention Policy rules

4. Storage & Encryption

- All backups and archives must be encrypted at rest.
- Transfer of backups to off-site or cloud storage must use secure channels (e.g. SFTP, TLS, VPN).
- Access to backups/archives restricted to authorized personnel only; access must be logged and audited.

5. Restoration & Recovery Testing

- Perform full restoration tests at least once per quarter to validate backup integrity and recovery procedures.
- Document test results, including restoration time, data integrity, and any issues encountered.

6. Archiving & Purging Procedures

- Once backup retention period expires (and no legal/contractual hold exists), delete or securely purge backups.
- Archived data must remain encrypted and access-controlled; only approved roles may retrieve.
- Keep audit logs for backup/archive and purge actions (who, when, what, why).

7. Roles & Responsibilities

- **IT / DevOps Team:** schedule and perform backups, manage storage, encryption, archiving, and restoration tests.
- **Project / Data Owners:** approve long-term archives for project deliverables, critical data, or compliance-related archives.
- **Security / Compliance Manager:** audit backup/archive practices, verify compliance with policies, handle legal/contractual holds or requests.

8. Policy Review & Update

- Review at least annually or when infrastructure, services, or volume changes significantly.
- Maintain version history, change log, and communicate updates to relevant teams.