

MarocAgency — Access Control & Authentication Policy

Version: 1.0

Effective Date: 2025-12-03

Approved by: IT Director / Security Manager

1. Purpose

Establish secure and standardized management of user accounts, authentication, permissions, and access control across all MarocAgency systems — to protect data confidentiality, integrity, and ensure accountability.

2. Scope

Applies to all systems, applications, cloud services, repositories, internal tools, data storage used by MarocAgency — accessed by employees, contractors, subcontractors, or external partners.

3. Access Control Principles

- Use **Role-Based Access Control (RBAC)**: permissions are granted based on roles and business need.
- Apply **least privilege** and **need-to-know** principles: users get only the minimum permissions required for their tasks.
- Perform **permission review** at least every 6 months — adjust, revoke, or re-validate roles as needed.

4. Authentication & Account Lifecycle

- Passwords must meet complexity requirements (minimum 12 characters, mixture of uppercase, lowercase, digits, special characters) or use secure passphrases.
- All accounts accessing sensitive data, production systems, or admin functions must use **Multi-Factor Authentication (MFA)**.
- Passwords must be changed every 90 days; reuse of old passwords is disallowed.
- Account lockout after 5 failed login attempts; requires manual reset.

Account Lifecycle Procedures

- **Onboarding:** identity verification, least-privilege assignment, logging of account creation.
- **Role changes:** promptly adjust permissions, revoke unnecessary rights.
- **Offboarding:** disable account within **1 hour** of employee/contractor departure; revoke credentials; recover company devices; audit to ensure no lingering access.

5. Logging & Monitoring of Access

- Log all access to sensitive/Confidential data and critical systems (user, timestamp, action, resource).
- Store logs securely with restricted access, following Data Retention Policy retention periods.
- Perform monthly reviews of logs for suspicious activity (unusual access times, failed logins, privilege escalations).
- Configure alerts for anomalous actions (e.g. repeated failed logins, admin-level actions during off-hours).

6. Temporary & Emergency Access

- Temporary elevated or emergency access must be requested in writing, with justification, limited duration, and logged.
- Emergency access must be revoked immediately after use and reviewed by Security Manager.
- Shared or generic accounts are prohibited; each user must have unique credentials.

7. Exceptions & Special Cases

- Any exception to this policy must be documented, justified, approved by Security Manager, and reviewed periodically.
- Administrative or privileged roles must be assigned only to senior or trusted staff.

8. Policy Review & Maintenance

- Review this policy at least every 6 months, or sooner if systems/organization change significantly.
- Maintain version history, change log, and approval records.