

Remote Access Policy

Document Title: Remote Access Policy

Version: 1.0

Prepared by: Muneer Shaukath

Next Review Date:

1. Purpose

To define requirements for secure remote access to the Emirates Face Recognition's internal network, systems, and data, protecting information assets against unauthorized access, data leakage, and misuse.

2. Scope

This policy applies to:

- All employees, contractors, third-party users, and vendors who remotely connect to the organization's network.
- All devices (company-owned or BYOD) used for remote access.

3. Policy Requirements

3.1 Authorized Access

- Remote access must be explicitly authorized by IT management.
- Access must be granted on a least-privilege basis.
- Users must sign confidentiality and acceptable use agreements.

3.2 Secure Connection Methods

- Remote connections must use secure channels such as VPN with strong encryption (e.g., IPsec or SSL/TLS).
- Multi-Factor Authentication (MFA) must be enforced for all remote connections.
- Default remote access protocols must be disabled if not in use (e.g., RDP, Telnet).

3.3 Device Security Requirements

- Devices must have updated antivirus and endpoint protection.
- Devices must be patched with the latest security updates.
- Personal devices must comply with BYOD security controls.

3.4 User Responsibilities

- Users must not share their credentials.
- Users must report lost or stolen devices immediately.
- Users must disconnect remote sessions when not in use.

3.5 Monitoring and Logging

- All remote access sessions must be logged and monitored.
- Logs must be retained according to the log retention policy.

3.6 Third-Party Access

- Third-party connections must be time-bound and reviewed regularly.

4. Non-Compliance

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

5. Roles and Responsibilities

Role	Responsibility
IT Security Manager	Approve and manage remote access configurations.
System Administrators	Implement secure access controls.
Users	Comply with this policy.
HR / Legal	Enforce disciplinary measures if required.

6. Review and Maintenance

This policy must be reviewed at least annually or when significant changes to systems or business processes occur.

Approval

Name	Position	Date	Signature
Sherry George	Technical Manager		_____

--End of Document--