Multi-Factor Authentication Policy for Telecommuters

1. Purpose

The purpose of this policy is to establish requirements for Multi-Factor Authentication (MFA) for all telecommuters accessing company systems, data, or networks from remote locations to ensure the security of organizational resources.

2. Scope

This policy applies to all employees, contractors, and third-party personnel who telecommute and require access to the organization's systems, applications, or data remotely.

3. Policy

1. **MFA Requirement:** All remote access to company systems must be authenticated using MFA. This includes, but is not limited to, VPN, email, corporate applications, and cloud services.
2. **Accepted MFA Methods:**
   - Authenticator app (e.g., Google Authenticator, Microsoft Authenticator)
   - Hardware security token
   - SMS/Phone call verification
   - Biometric authentication (where supported)
3. **Password Policies:** Users are required to use strong and unique passwords in combination with MFA.
4. **Device Security:** Devices used for MFA must be secured with a password or biometric lock.
5. **Reporting:** Any suspected breach or compromise of authentication devices must be reported to IT immediately.

4. Roles and Responsibilities

Role	Responsibilities
Telecommuters	Comply with MFA policy and report lost or compromised authentication devices.
IT Department	Implement, monitor, and support MFA technologies; provide user support and awareness training.
Managers	Ensure team compliance and address non-conformance.

5. Enforcement

Failure to comply with this policy may result in disciplinary action, including suspension of access privileges, and where appropriate, legal action.

6. Policy Review

This policy will be reviewed annually by IT Security to ensure its effectiveness and relevance.

7. Acknowledgment

All telecommuters must acknowledge their understanding and acceptance of this policy prior to remote access being granted.