📝 Remote Work Security Policy

Version: 1.0
Effective Date: April 2025

Purpose

To define standards and procedures for maintaining data security while working remotely, ensuring that all employees, contractors, and partners understand their responsibilities.

Scope

Applies to all users performing work functions from remote locations using company-issued, CYOD, or BYOD devices.

Policy

- All remote connections to internal resources must occur over a company-approved VPN.
- Use of MFA is mandatory for all authentication processes.
- Devices used remotely must have:
  - Active antivirus/antimalware
  - Full-disk encryption
  - Device lockout after 10 minutes of inactivity
- Use of shared or public computers for company work is strictly prohibited.
- All files should be saved to company-approved cloud storage, not locally.
- Screen-sharing and video conferencing tools must be company-vetted and access-controlled.

Device Requirements

- Company-issued/CYOD devices must be updated regularly by IT.
- BYOD devices must be enrolled in MDM and pass regular compliance checks.

Reporting

Security incidents (e.g., device theft, suspicious activity) must be reported within 1 hour to IT/ Security.

Enforcement

Failure to comply with this policy may result in disciplinary action or access restrictions.