# REMOTE ACCESS POLICY

Version: 1.0

Date: July 22, 2025

Author: Luis Echeverria

Organization: [organization name]

## 1. Purpose

This Remote Access Policy defines the standards and requirements for securely connecting to the organization's network from remote locations. The goal is to protect sensitive information and maintain secure communication channels.

## 2. Scope

This policy applies to all employees, contractors, and third-party vendors who require access to internal systems from external locations using personal or company-issued devices.

## 3. Authorized Methods

All remote access must be conducted through secure methods, including:

* - VPN (Virtual Private Network) with encryption
* - Multifactor authentication (MFA)
* - Approved remote desktop tools or gateways

## 4. Device Requirements

Devices used for remote access must:

* Have up-to-date antivirus and antimalware software
* Use supported and patched operating systems
* Be configured to automatically lock after inactivity
* Not be shared with unauthorized users

## 5. User Responsibilities

* Only access systems necessary for job functions
* Report lost or stolen devices immediately
* Avoid using public Wi-Fi without a secure VPN
* Refrain from downloading sensitive data unless authorized

## 6. Monitoring and Logging

Remote access sessions may be monitored and logged to ensure compliance and detect unauthorized activity.

## 7. Enforcement

Non-compliance with this policy may result in access revocation, disciplinary action, or legal consequences depending on the severity.

## 8. Review

This policy will be reviewed annually or in response to changes in remote work practices or security threats.

Approved by: [Insert Name or Role]

Review Date: [Insert Future Review Date]