Remote Access Policy

Remote Access Requirements

SA

Secured approach  www.securedapproach.com

Use Disclaimer: This policy has been developed by Secured Approach Inc. for the benefit of the community. You are welcome to use this policy, in whole or in part, for your organization without the need for prior approval. Should you wish to contribute to creating or updating a new version of this policy, please reach out to us via email at resources@securedapproach.com.
Furthermore, if you require assistance in crafting a tailored security policy for your specific environment, do not hesitate to contact us at support@securedapproach.com.

Table of Contents

[Confidentiality Statement 2](#_Toc159342207)

[Disclaimer 2](#_Toc159342208)

[1. Overview 2](#_Toc159342209)

[2. Purpose 2](#_Toc159342210)

[3. Scope 2](#_Toc159342211)

[4. Policy 3](#_Toc159342212)

[4.1 Connection Requirements 3](#_Toc159342213)

[4.2 Technology Requirements 3](#_Toc159342214)

[4.3 Authentication Requirements 3](#_Toc159342215)

[4.4 Monitoring and Logging 3](#_Toc159342216)

[5. Policy Compliance 3](#_Toc159342217)

[5.1 Compliance Measurement 3](#_Toc159342218)

[5.2 Exceptions 4](#_Toc159342219)

[5.3 Non-Compliance 4](#_Toc159342220)

[6. Related Standards, Policies, and Processes 4](#_Toc159342221)

[7. Revision History 4](#_Toc159342222)

# Confidentiality Statement

This document is confidential and intended solely for the use of [Organization Name]'s employees and authorized individuals. Unauthorized sharing, distribution, or reproduction of this document or its contents is strictly prohibited and may lead to disciplinary actions.

# Disclaimer

This Remote Access Policy is subject to change at any time to adapt to new technologies, threat landscapes, and best practices. It is the responsibility of all users to stay informed of these changes and comply accordingly.

# Overview

The Remote Access Policy outlines the standards and conditions under which employees and authorized individuals can access [Organization Name]'s network and resources remotely. This policy is designed to minimize the risk of data breaches, unauthorized access, and other cyber threats.

# Purpose

To ensure the security of [Organization Name]'s data and technology infrastructure by establishing guidelines for secure remote access to the organization's network and systems.

# Scope

This policy applies to all employees, contractors, and third-party service providers of [Organization Name] who have been granted remote access to the organization’s network and systems.

# Policy

## Connection Requirements

* Remote access must be performed through secure, encrypted connections such as VPNs with up-to-date security protocols.
* Remote users are prohibited from connecting to the organization’s network via public or unsecured Wi-Fi networks.

## Technology Requirements

* Only approved software and devices may be used to establish remote connections. This includes maintaining up-to-date antivirus software and a firewall on the remote device.
* The transfer of sensitive information to personal devices is strictly forbidden. Remote access from personal or non-organization-owned devices must comply with the organization's device security standards.

## Authentication Requirements

* Users must utilize strong passwords and multi-factor authentication (MFA) to access the organization’s systems remotely.
* Use of privileged or administrative accounts must follow stricter password and authentication requirements and is subject to tighter scrutiny and controls.
* Sharing of remote access credentials is strictly prohibited. Each user is responsible for the actions performed with their credentials.

## Monitoring and Logging

* All remote access activities must be logged, and the organization reserves the right to monitor and audit remote access sessions.

# Policy Compliance

## Compliance Measurement

Regular audits will be conducted to ensure compliance with this policy. This includes reviewing remote access logs and user activities.

## Exceptions

Any exceptions to this policy due to compatibility issues or limitations must be submitted in writing with a business justification and approved by the IT Security Department or relevant authority within the organization.

## Non-Compliance

Violations of this policy may result in disciplinary action, up to and including termination of access, employment, legal action, and financial liabilities.

# Related Standards, Policies, and Processes

* Acceptable Use Policy
* Data Protection Policy
* Identity and Access Management Policy

# Revision History

This policy will be reviewed and updated annually or as needed to reflect changes in technology, legal requirements, and organizational priorities. The revision history will be documented here, including the date of the revision, a brief description of the changes, and the version number.

|  |  |  |  |
| --- | --- | --- | --- |
| Date of Change | Responsible | Summary of Change | Version |
| January 2024 | Information Security Manager | Building the first draft | 1.0 |
| January 2024 |  |  |  |
|  |  |  |  |