# [Company Name] Remote Access Policy and Procedures

| | |
|---|---|
| ***Official Policy Title:*** | |
| ***Responsible Party:*** | |
| ***Approval Party:*** | |
| ***Effective Date:*** | |
| ***Last Update:*** | |
| ***Version Number:*** | |
| ***Policy Framework:*** | **Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800 (NIST SP 800-53, rev. 5)** |
| ***Mapping*** | **(1). NIST SP 800-53, rev. 5 (AC-17).** |

## Introduction

The Remote Access policy and procedures referenced within this document defines the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Remote Access policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

## Purpose

The purpose of the Remote Access policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*
- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

## Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

## Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

**Remote Access Platform**

The [company name] remote access platforms utilized for accessing information systems are to consist of communication protocols, and other supporting devices that ultimately ensure the confidentiality, integrity, and availability (CIA) of such a connection, along with the organization's network. This means using secure connectivity methods utilizing appropriate levels of encryption, such as SSL and IPSec VPN tunneling, and other approved methods. Remote access platforms that do not meet these minimum requirements are strictly forbidden.

| Remote Access Protocol | Description | Encryption Protocol Used [NIST-AC-17(2)] | Environment Accessed |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Authorized Users**

The use of remote access is a privilege - one that is to be assigned only to authorized individuals with a justified business need for such access - and only after comprehensive analysis and subsequent approval procedures have been undertaken by applicable supervisory personnel and all necessary I.T. authorities. Additionally, a documented and formalized provisioning process is to be undertaken, which requires the completion of the Remote Access Request Form (form), along with acknowledgement and signature by all parties, including the user. By signing the form, users agree to abide by all stated policies and procedures for ensuring the safety and security of remote access connections, and to whichever network(s) being connected to.

Depending on the type of remote access given, [company name] I.T. personnel will set up, establish, and enable all necessary technical and security configurations for such access, which includes, but is not limited to, enrolling users into specific systems, configuring remote access "client" software on applicable machines, assigning username and passwords, and other necessary measures. Lastly, users terminated by [company name] are to have their remote access rights immediately revoked.

**Usernames and Passwords**

Unique usernames and passwords that meet or exceed stated best practices for complexity rules are to be implemented for all users with remote access rights. Also, stated lockout times for idle remote access sessions, along with predefined time parameters (i.e., 180 minutes, etc.) for allowing such access rights are to be configured accordingly. Because remote access procedures often require authenticating through different access points, strong passwords are to be enforced at all times.

System: [Name of system being used to authenticate against for remote access (i.e., MS Active Directory, actual website URL, etc.)

- Password parameters and complexity rules for remote access client/platform consist of the following:
- Password Parameters:
- Passwords must be masked - yes or no.
- Passwords must have special character(s), defined as [ ]
- Passwords must conform to minimum length requirements, which are stated as [ ].
- Passwords must conform to minimum history requirements from being re-used, which are stated as [ ].
- User Accounts locked after [ ] number of invalid login attempts.
- Users access locked out after [ ] minutes of computer activity.

Additionally, users are forbidden to share such privileged account information with anyone else, both internally within the organization, and externally. Users are also forbidden from displaying their usernames and passwords in any manner that can allow other individuals to capture such information and gain access to the [company name] network. Social engineering is a growing threat, and all users are to be keenly aware of various tactics that can be utilized to obtain such privileged information.

**Two-Factor Authentication**

Because of the different types of remote access mediums and protocols allowed, along with the numerous devices that can be used for initiating remote access sessions, the following security measures are to apply:

- Remote access client software – if residing on a user's device – is not to be altered in any way.
- Personal firewalls software must be enabled on computers, along with other malware protection measures, such as a current, known, and stable version of antivirus.

- Along with not altering remote access client software, users are also forbidden from altering and changing any configurations on [company name] information systems that would affect the security of such systems, and also the remote access session.
- Users are forbidden from initiating remote access sessions from untrusted end-user devices that are not owned, operated, maintained, and controlled by [company name] and pose a serious security threat. Common examples include, but are not limited to, the following: mall kiosks that offer Internet services, hotel business/computer rooms offering pc's for use, office supply/mailing stores providing computers for printing, faxing, scanning services, etc.
- Users are forbidden from engaging in dual connectivity/concurrent connectivity, whereby a user is connected to the [company name] network, while also on another network.
- Remote access rights are strictly for authorized users who have been assigned such rights, and not for any other individuals, such as personal friends, family members, co-workers, etc.
- Confirmation of remote session termination, such as closing out of the program and the browser, is to be conducted after each session. As a security precaution, [company name] has implemented a predetermined "time-out" clause for remote access to help increase security.

In summary, the same consideration that is given to a user's onsite connection to the [company name] network must also be utilized for remote access sessions. Additionally, users are to display reasonable and prudent security measures for ensuring the physical safety of any [company name] devices for establishing remote access sessions. This would include, but not limited to, not leaving laptops in untrusted environments, safely securing devices when in public domains, etc.

**Patch Management**

It is the responsibility of [company name] I.T. personnel to ensure that all information systems that facilitate and administer remote access rights are current with all applicable security upgrades and patches. This would include all network level patches, operating system and application patches, along with necessary anti-virus, personal firewall software, and other necessary protocols for end-user systems as previously mentioned.

**Security Incidents**

Should a user suspect or confirm that an actual security issue has arisen relating to one's remote access session, such user is to terminate the remote access session and report the incident immediately to authorized I.T. personnel. Additionally, the user is to make available any company-owned and personally owned, operated, maintained, and controlled assets (i.e., laptops, key fobs, USB drives, etc.) to [company name] immediately for purposes of possible forensic analysis. Any data or information viewed or retrieved during the remote access session is to be analyzed also for possible security issues.

**Business Use Only**

Remote access is a privilege, thus all authorized users are to utilize such services for business use only, with no personal or questionable activities allowed. "Business use only" implies the following: (1). for facilitating all required duties for a stated job function, (2). for communicating with other authorized parties (i.e., employees, clients, contractors, etc.), (3). for conducting research applicable to one's job

duties. Data and information accessed is often highly sensitive and confidential, requiring due professional care at all times, which means no “co-mingling” with personal activities that could jeopardize the safety and security of [company name] assets.

Specifically, the following are strictly forbidden when utilizing [company name] remote access rights:

- Visiting personal websites, such as email accounts, social media sites, and other websites not deemed professional in nature or part of one’s job duties.
- Engaging in any illegal activities, threats, harassments, defamation, slander, along with posting comments or sending communication that suggests or implies such behavior.

In summary, users are accountable for all activities conducted while connected to the [company name] network through remote access rights.

**Confidential Information**

Personal and confidential information is never allowed to be stored on any local devices used for enabling a remote session, such as one’s hard drive, or using external storage devices via USB connections. Because personal and confidential information is often labeled as Personally Identifiable Information PII), great care and consideration must be taken for ensuring the safety and security of such data.

Additionally, [company name] also reserves the right to periodically inspect devices used by users for initiating remote access sessions for ensuring no such data is found. From a technical perspective, information is an ordered sequence of symbols, along with a concept well-associated with the likes of communication, data, knowledge, meaning, etc. Moreover, "information" can also be interpreted as material that can be viewed or manipulated in a manner for which it provides a logical and meaningful output.

**Monitoring and Control** [NIST-AC-17(1)], [NIST-AC-17(3)],

[Company name] reserves t[illegible] without consent, which may include installing agent soft[illegible], performance, and overall monitoring issues. The confidentiality, integrity, and availability (CIA) of [company name]’s network [illegible]