**Remote Access Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_4r9rufe2ptoh) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_bce16ihdh2mo) **3**

[**Scope**](#_3dy6vkm) **4**

[**Policy**](#_1t3h5sf) **4**

[**Prohibited Actions**](#_q56tuhioqkcw) **4**

[**Network Access**](#_ilravuqv61jr) **4**

[**Connections and re-authentication**](#_7sj8achcter8) **4**

[**Disciplinary actions**](#_oo4pebgvtuk2) **5**

[**Change, Review, and Update**](#_6cu0cv3y3y7n) **5**

[**Responsibility**](#_fxvzxllev4xj) **5**

[**Reference**](#_1ksv4uv) **5**

[**Related Documents**](#_oqj2g9kzbmil) **5**

# Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc.

# Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses [*Company]* information assets or information resources and services.

# Policy

## Prohibited Actions

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically prohibited:

* Installing a modem, router, or other remote access device on a company system without the approval.
* Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the approval.
* Use of non-company-provided remote access software.
* Split Tunneling to connect to an insecure network in addition to the corporate network, or in order to bypass security restrictions.

## Network Access

* There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.

## Connections and re-authentication

* Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the company's network must be timed out after 1 hour of inactivity and re-authentication will be required every 24 hours.

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how serious an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# Related Documents

* UD Password Management Policy