

# Remote Access Policy

Last updated: November 2023

## 1. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks the best of our ability.

## 2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Cloudoko's network from any host. These rules and requirements are designed to minimize the potential exposure to Cloudoko from damages which may result from unauthorized use of Cloudoko resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Cloudoko internal systems, and fines or other financial liabilities incurred as a result of those losses.

## 3. Scope

This policy applies to all Cloudoko employees, contractors, vendors and agents with a Cloudoko-owned or personally-owned computer or workstation used to connect to the Cloudoko network. This policy applies to remote access connections used to do work on behalf of Cloudoko, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Cloudoko networks.

## 4. Policy

It is the responsibility of Cloudoko employees, contractors, vendors and agents with remote access privileges to Cloudoko's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Cloudoko.

General access to the Internet for recreational use through the Cloudoko network is strictly limited to Cloudoko employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Cloudoko network from a personal computer, Authorized Users are responsible for preventing access to any Cloudoko computer resources or data by non-Authorized Users. Performance of illegal activities through the Cloudoko network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use Cloudoko networks to access the Internet for outside business interests.

### Requirements

1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Protection Policy.
2. Authorized Users shall protect their login and password, even from family members.
3. While using a Cloudoko-owned computer to remotely connect to Cloudoko's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
4. Use of external resources to conduct Cloudoko business must be approved in advance by InfoSec and the appropriate business unit manager.
5. All hosts that are connected to Cloudoko internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

## 5. Policy Compliance

### Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6. Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Cloudoko's network:

- [Acceptable Encryption Policy](#)
- [Acceptable Use Policy](#)
- [Password Protection Policy](#)

## 7. Definitions and Terms

None.

## 8. Revision History

Date of Change	Responsible	Summary of Change
November 2023	Kevin Boldy	Initial Version



[www.cloudoko.com](http://www.cloudoko.com)