**Remote Access Policy**

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 College network. While these remote networks are beyond the control of Rocky Mountain College’s policy, we must mitigate these external risks the best of our ability.

1. **Purpose**

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

1. **Scope**

This policy applies to all Rocky Mountain College employees, contractors, vendors and agents with a College-owned or personally-owned computer or workstation used to connect to the College network. This policy applies to remote access connections used to do work on behalf of Rocky Mountain College, 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 Rocky Mountain College’s networks.

1. **Policy**

It is the responsibility of Rocky Mountain College’s employees, contractors, vendors and agents with remote access privileges to the network to ensure that their remote access connection is given the same consideration as the users on-site.

General access to the Internet for recreational use through the Rocky Mountain College’s network is strictly limited to Rocky Mountain College’s employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the network from a personal computer, Authorized Users are responsible for preventing access to any computer resources or data by non-Authorized Users. Performance of illegal activities through the College 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 Rocky Mountain College’s networks to access the Internet for outside business interests.

* 1. **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 Policy.
    2. Authorized Users shall protect their login and password, even from family members.
    3. While using a Rocky Mountain College-owned computer to remotely connect to College’s 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.
    4. Use of external resources to conduct College business must be approved in advance by InfoSec manager and the Director.
    5. All hosts that are connected to Rocky Mountain College’s internal networks via remote access technologies must use the College provided computer with the latest anti-virus/Zero trust software.

1. **Policy Compliance**
   1. **Compliance Measurement**The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.
   2. **Exceptions**Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.
   3. **Non-Compliance**An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
2. **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 Rocky Mountain College’s network:

* Acceptable Encryption Policy
* Computer Use Policy
* Password Policy