**Employee Internet Use Monitoring and Filtering Policy**

1. **Overview**

See Purpose.

1. **Purpose**

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within Rocky Mountain College’s network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

1. **Scope**

This policy applies to all Rocky Mountain College’s employees, contractors, vendors and agents with a College-owned or personally-owned computer or workstation connected to the College’s network.

This policy applies to all end user initiated communications between Rocky Mountain College’s network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

1. **Policy**
	1. **Web Site Monitoring**

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server.

Internet Use records must be preserved for 30 days.

* 1. **Access to Web Site Monitoring Reports**

The Infosec Security Incident Response Team (ISIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the ISIRT upon written or email request to the Infosec Manager from a Human Resources Representative.

* 1. **Internet Use Filtering System**

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Rocky Mountain College’s environment. The following protocols and categories of websites should be blocked:

* Command and Control
* Copyright Infringement
* Dynamic DNS
* Extremism
* Gambling
* Grayware
* Hacking
* Malware
* Newly Registered Domains
* Parked
* Peer to Peer File Sharing
* Phishing
* Private IP Addresses
* SPAM, Phishing and Fraud
* Spyware
* Web Advertisements
	1. **Internet Use Filtering Rule Changes**

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Usage Policy.

* 1. **Internet Use Filtering Exceptions**

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to Human Resources. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site and will track approved exceptions and report on them upon request.

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 feedback to the policy owner.
	2. **Exceptions**Any exception to the policy must be approved by 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**

None.