**Cyber Security Policy**

1. **Overview**

Cyber security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of Rocky Mountain College. The goal of the Cyber Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within Rocky Mountain College while providing value to the way we conduct business.

Protection of the Confidentiality, Integrity, and Availability are basic principles of Cyber Security, and can be defined as:

* Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic “need-to-know” principle.
* Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
* Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Rocky Mountain College has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security(Infosec) policies may be developed to ensure that the college can efficiently and effectively manage, control and protect its information assets and those information assets entrusted to Rocky Mountain College by its students, partners, and other third-parties.

The College’s Cyber Security Program is built around the information contained within this policy and its supporting policies.

1. **Purpose**

The purpose of the Rocky Mountain College’s Cyber Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Rocky Mountain College, its business partners, and its students.

1. **Scope**

The Rocky Mountain College Cyber Security Policy applies equally to all employees, contractors, consultants, work study, and other individuals that interacts with any College Information Resource.

* 1. **Responsibilities**

**President’s Cabinet**

* Ensure that an appropriate risk-based Cyber Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Rocky Mountain College.
* Ensure that Cyber security processes are integrated with strategic and operational planning processes to secure the college’s mission.
* Ensure adequate Cyber security financial and personnel resources are included in the budgeting and financial planning process.
* Ensure that the Infosec Team is given the necessary authority to secure the Information Resources under their control within the scope of Rocky Mountain College’s Cyber Security Program.
* Designate an Infosec Manager and delegate authority to that individual to ensure compliance with applicable Infosec requirements.
* Ensure that the Infosec Manager, in coordination with the Infosec Team, reports annually to President’s Cabinet on the effectiveness of the college’s Infosec Program.

**Infosec** **Security Manager**

* Chair the Infosec Team and provide updates on the status of the Infosec Program to the President's Cabinet.
* Manage compliance with all relevant statutory, regulatory, and contractual requirements.
* Participate in security related forums, associations and special interest groups.
* Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Rocky Mountain College.
* Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
* Ensure that Rocky Mountain College has trained all personnel to support compliance with Infosec policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for Infosec with respect to such responsibilities.
* Ensure that appropriate Infosec awareness training is provided to Rocky Mountain College employees, consultants, work studies, and other individual, including contractors.
* Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the Infosec policies, procedures, and practices of Rocky Mountain College.
* Develop and implement procedures for testing and evaluating the effectiveness of the College’s Infosec Program in accordance with stated objectives.
* Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.
* Report annually, in coordination with the Infosec Team, to the President’s Cabinet on the effectiveness of Rocky Mountain College’s Infosec Program, including progress of remedial actions.

**Infosec** **Team**

* Ensure compliance with applicable Infosec requirements.
* Formulate, review and recommend Infosec policies.
* Approve supporting procedures, standards, and guidelines related to Infosec.
* Provide clear direction and visible management support for Infosec initiatives.
* Assess the adequacy and effectiveness of the Infosec policies and coordinate the implementation of information security controls.
* Ensure that ongoing security activities are executed in compliance with policy.
* Review and manage the Infosec policy waiver request process.
* Review Infosec incident information and recommend follow-up actions.
* Promote Infosec education, training, and awareness throughout Rocky Mountain College, and initiate plans and programs to maintain Infosec security awareness.
* Report annually, in coordination with the Infosec Manager, to the President’s Cabinet on the effectiveness of Rocky Mountain College’s Infosec Program, including progress of remedial actions.
* all employees, contractors, consultants, work study, and contractors
* Understand their responsibilities for complying with Rocky Mountain College’s Infosec Program.
* Use Rocky Mountain College’s Information Resources in compliance with all Infosec Policies.
* Seek guidance from the Infosec Team for questions or issues related to information security.
1. **Policy**

Rocky Mountain College maintains and communicates a Cyber Security Program consisting of topic-specific policies, standards, procedures and guidelines that:

* Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the college using administrative, physical and technical controls.
* Provide value to the way we conduct business and support institutional objectives.
* Comply with all regulatory and legal requirements, including:
	+ FERPA Security Rule,
	+ State breach notification laws,
	+ PCI Data Security Standard,
	+ Information Security best practices, including ISO 27002 and NIST CSF,
	+ Contractual agreements,
	+ All other applicable federal and state laws or regulations.

The cyber security program is reviewed no less than annually or upon significant changes to the Infosec environment.

1. **Policy Compliance**
	1. **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.

* 1. **Exceptions**

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

* 1. **Non-Compliance**

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

1. **Reference Documents**
	1. **Rocky Mountain College Policy or Guideline**
* Acceptable Encryption Policy
* Anti-Virus Guidelines
* Computer User Policy
* Data Breach Policy
* E-mail Policy
* Employee Internet use Monitoring and Filtering Policy
* Gramm-Leach-Bliley Act Policy
* Internet Use Policy
* Password Construction Guideline
* Password Protection Policy
* Remote Access Mobil Computing Storage Policy
* Remote Access Policy
* Removable Media Policy
* Software Installation Policy
	1. **External Resources**
* Code of practice for Information security management; ISO 27002
	+ https://www.iso.org/standard/54533.html
* National Institute of Standards and Technology Cyber Security Framework
	+ https://www.nist.gov/cyberframework
* Family Educational Rights and Privacy Act (FERPA)
	+ https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
* Gramm-Leach-Bliley Act (GLBA)
	+ https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act
* Payment Card Industry Data Security Standard (PCI DSS)
	+ <https://www.pcisecuritystandards.org/document_library>