**Data Breach Response Policy**

1. **Overview**
2. **Purpose**

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Rocky Mountain College’s Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Rocky Mountain College’s established culture of openness, trust and integrity should respond to such activity. Rocky Mountain College’s Information Security is committed to protecting our employees, partners and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

1. **Background**

This policy mandates that any individual who suspects that a theft, breach or exposure of Rocky Mountain College’s Protected data or Sensitive data has occurred must immediately provide a description of what occurred via e-mail to support@rocky.edu, by calling (406)657-1161, or calling (406)238-7360. This e-mail address, and phone numbers are monitored by the Rocky Mountain College’s Infosec team. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Infosec manager will follow the appropriate procedure in place.

1. **Scope**

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or sensitive data belonging to Rocky Mountain College. Any agreements with vendors will contain language similar that protects the fund.

1. **Policy**
	1. Confirmed theft, data breach or exposure of Rocky Mountain College’s Protected data or Sensitive data

	As soon as a theft, data breach or exposure containing Rocky Mountain College Protected data or Sensitive data is identified, the process of removing all access to that resource will begin.

	The Infosec Manager will chair an incident response team to handle the breach or exposure.

	The team will include members from:
* IT
* Finance (if applicable)
* Communications
* Student Services (if student data is affected)
* Human Resources
* The affected department that uses the involved system or output or whose data may have been breached or exposed
* Additional departments based on the data type involved, additional individuals as deemed necessary by the Infosec Manager

The President will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

**Work with Forensic Investigators**
As provided by EIIA cyber insurance, Rocky Mountain College will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

**Develop a Communication Plan**

Work with Rocky Mountain College’s communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

* 1. Ownership and Responsibilities
		1. Roles & Responsibilities:
* Sponsors are those members of the Rocky Mountain College’s community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Rocky Mountain College Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
* Infosec Manager is that member of the Rocky Mountain College community, designated by the President’s cabinet, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
* Users include virtually all members of the Rocky Mountain College’s community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees, work studies, and volunteers.
* The Incident Response Team shall be chaired by the Infosec Manager and shall include, but will not be limited to, the following departments or their representatives: IT, Communications; Management; Financial Services, Student Services; Human Resources.
1. **Enforcement**

Any Rocky Mountain College personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.