**Remote Access Mobile Computing Storage Policy**

1. **Overview**

With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs at the Rocky Mountain College. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at the Rocky Mountain College.

1. **Purpose**

The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access information resources at the Rocky Mountain College.

1. **Scope**

Rocky Mountain College’s employees, consultants, vendors, contractors, work study students, and others who use the College’s mobile computing and storage devices.

1. **Policy**
	1. **General Policy**

It is the policy of the Rocky Mountain College that mobile computing and storage devices containing or accessing the information resources at the College must be approved prior to connecting to the information systems. This pertains to all devices connecting to the information resources, regardless of ownership.

Mobile computing and storage devices include, but are not limited to: laptop computers, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or Rocky Mountain College owned, that may connect to or access the information systems at the College. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at the College unless the media type has already been approved by Infosec. Infosec will maintain a list of approved mobile computing and storage devices.

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at the College. These risks must be mitigated to acceptable levels.

Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive Rocky Mountain College information must use encryption at rest or equally strong measures to protect the data while it is being stored.

Unless written approval has been obtained from the Information Security Officer, databases or portions thereof, which reside on the network at the Rocky Mountain College, shall not be downloaded to mobile computing or storage devices.

* 1. **Procedures**

To report lost or stolen mobile computing and storage devices, call the Help Desk.

The Infosec Committee shall approve all new mobile computing and storage devices that may connect to information systems at the College.

Any non-departmental owned device that may connect to the College’s Information Systems must first be approved by Infosec personnel. Refer to the Mobile Media Standards for detailed information.

* 1. **Roles & Responsibilities**

Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by the College. Before connecting a mobile computing or storage device to the Information systems at Rocky Mountain College, users must ensure it is on the list of approved devices issued by Infosec.

The Help Desk must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

The Infosec team is responsible for the mobile device policy at the Rocky Mountain College and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by the Rocky Mountain College.

The Infosec team is responsible for developing procedures for implementing this policy, and will maintain a list of approved mobile computing and storage devices.

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.

* 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. **Related Standards, Policies and Processes**

None.