**Removable Media Policy**

1. **Overview**

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

1. **Purpose**

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Rocky Mountain College and to reduce the risk of acquiring malware infections on computers operated by Rocky Mountain College.

1. **Scope**

This policy covers all computers and servers operating in Rock Mountain College.

1. **Policy**

Rocky Mountain College staff may only use Infosec approved/provided removable media in their work computers. Rocky Mountain College removable media may not be connected to or used in computers that are not owned or leased by Rocky Mountain College without explicit permission of the Infosec staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Rocky Mountain College’s *Acceptable Encryption Policy*.

Exceptions to this policy may be requested on a case-by-case basis by Rocky Mountain College’s exception procedures.

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**
   1. Acceptable Encryption Policy