# Removable Media Policy

## Overview

Removable media takes many forms today (jump drives, flash memory storage, portable storage devices, etc.). Removable media is personal, removable, and portable which introduces risk into the organization whenever it is used to store sensitive information. Aside from the chance for loss and theft, removable media format storage is a well-known source of malware infections and has been directly tied to the loss of information.  
  
2. Purpose

This policy is established to minimize the risk of loss or exposure of sensitive maintained by [LEP] as well as reducing exposure to external sources of malware and virus exploit in the [LEP] environment.

## Scope

This policy applies to all [LEP] staff using [LEP] resources.

## Policy

### General

For the purposes of definition, the following items shall fall under the category of removable media:

* Flash (Jump) Drives and flash memory storage
* SD Storage
* Removable fixed drives and portable caddies
* R/W Compact Disk or DVD media
* USB remote storage devices

Removable media storage of any type shall generally be disallowed in any form or function within the [LEP] operational environment. Personal storage devices shall not be used for storage of any [LEP] information or be used with [LEP] hardware. Exceptions to this policy shall be considered only in unique and rare cases. These requests shall require written approval of the [Insert Appropriate Role] and be granted only for justifiable business purposes.

### Exception Policy

The [Insert Appropriate Role] or their designee shall ensure:

* Computer policy and procedures exist to scan all removable media when connected to a [LEP] asset and disallow saving of information to these devices under a normal user context
* Policy exception logs are maintained by the [LEP]
* Any removable media specifically approved for special case use shall be organizationally encrypted in a similar fashion to remote assets such as laptops
* Information saved to the device shall carry the same public-private key combination associated with the approved user
* For approved removable media policy exceptions, users of removable media shall ensure:
  + Media shall be backed up as part of the primary asset associated with the user
  + All [LEP] device backup and security protocols shall be followed and remain in place
  + Removable media may not be connected to, or used, in personal or home computers
  + Data shall be copied or stored on removable media only by authorized users in the performance of official duties
  + Removable media containing sensitive information shall have an external label that is marked and dated
  + Except for backups user shall prohibit copying, moving or storing sensitive data on local hard drives and removable media
  + Media containing information shall be protected against unauthorized access, misuse, or corruption
  + When in transit, sensitive data stored on removable media must not be left unattended and must remain in an authorized employee’s physical control at all times
  + Physical controls shall be provided for removable media containing sensitive information
  + Removable media shall be kept in a secure safe or a locked cabinet and returned to safe storage at the end of each work day
  + Staff shall adhere to the requirements applicable disposal policy and procedures when decommissioning removable media

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] internal procedures. Examples of suitable controls and practices include:

* Anecdotal exception and approval documents for staff requesting removable media access
* Computer group policy supporting removable media encryption and security controls
* On-demand operations logs for approved removable media users

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 12/02/2016 | Initial Policy Drafted |  |
|  |  |  |  |