**Overview**

Removable data drives (USB drives, flash drives, mobile hard drives, etc.) are a potential risk for accidental loss of sensitive information and a potential risk for nefarious acts of data theft. Beyond the loss prevention scope, removable data drives also present a risk of malicious attacks when infected removable devices are introduced to a network.

**Purpose**

The intent of this policy is to protect sensitive information by minimizing the risk of unsecure exposure of company data and preventing malicious exploits from being introduced to our network.

**Scope**

This policy applies to all staff and third party vendors that have authorization to use company owned computers and network resources.

**Policy**

1. General

For the purposes of definition, the following items fall under the removable data drive category.

* USB Drives
* Flash Drives
* Memory Cards
* External Hard Drives
* Hard Drive Caddies (Removable internal hard drives)
* DVD/CD writable media
* Smartphones

Removable data drives are restricted to authorized users that have a company issued removable

data drive. Personal removable data drives are not permitted for use on company owned

computers, laptops, or any other networked devices. A waiver for this policy may be considered

on a (temporary) case by case basis. A request for a waiver must be submitted in writing to the

(Chief Information Officer, etc.) for approval.

1. Exception Policy

The (Chief Information Officer, etc.) is responsible to ensure:

* Company owned computers are configured to deny write access to removable drives/media that are not encrypted.
* Waived removable data drives are encrypted and meet compliance standards.
* Policy waiver requests are retained, and recipients are notified when they expire.
* Users do not access the waived removable data drive on their personal computer.
* Users never leave removable data drives unattended, and they always maintain possession when company data is stored on the device.

**Enforcement**

Employees that violate this policy may be subject to disciplinary action, up to and including

possible termination.