**Removable Media Procedure**

Removable media (Flash Drives, External Hard Drives, Thumb Drives) are a well-known avenue for data loss and a source of malware infections.

# PurposeThe purpose of this procedure is to minimize the risk of loss or exposure of sensitive information maintained by the [Organization] and to reduce the risk of acquiring malware infections on computers operated by [Organization].

# Scope

# This procedure covers all computer devices and servers operating in the [Organization].

# Procedure

**[Organization]** staff may only use the **[Organization]** authorized removable media with their devices for work-related functions. Sensitive information generally should not be stored on removable media. If this is required for **[Organization]** work, it must be encrypted and placed only on officially registered removable media devices. Employees, contractors, and temporary staff will follow all [**Organization]** data removal procedures to permanently erase **[Organization]** -specific data from such devices once their use is no longer required. All users agree to immediately report to his/her manager and **[Organization]** any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of **[Organization]** resources, databases, networks, etc.

[**Department**] staff or the division administrator will distribute approved encrypted USB-based memory devices and related software applications and utilities. Devices that are not furnished by **[Department]** staff or the division administrator may not be connected to the **[Organization]** infrastructure.

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

The **[Department]** will verify compliance to this procedure through various methods, including but not limited to: periodic walk-throughs, business tool reports, internal and external audits, and device restrictions. **[Department]** reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to the **[Organization]** network. **[Department]** will engage in such action if equipment is being used in such a way that puts the **[Organization]’s** systems, data users and clients at risk.

# Exceptions

Limited exceptions to the procedure must be approved by the **[management]**.

1. **Definitions**

Removable Media: any or all of the following devices and technologies:

* Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives or key drives
* Memory cards in SD, CompactFlash, memory stick, or any related flash-based supplemental storage media
* USB card readers that allow connectivity to a PC
* Portal MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function
* PDAs, cell phone handsets, and Smartphones with internal flash or hard drive-based memory that support a data storage function
* Digital cameras with internal or external memory support
* Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks
* Any hardware that provide connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth among others) or wired network access