Office of the Chief Information Officer Directive: IT 13.07	Published: 04/2019
Chapter: User Responsibilities	Last Review: 01/2022
Subject: **Removable Media**	

1 DIRECTIVE

1.01 Users having a justifiable business reason for copying data to removable media and taking the media offsite must have their manager's written approval for using or transporting the removable media offsite.

1.02 The only removable media that may be used or connected to company equipment or networks are media that have been approved for use by IT Technical Support and either purchased by the company or approved for transfer into the ownership of the company.

1.03 Removable media must be handled, protected, reallocated and decommissioned as directed in the *Procedures* section below.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that, with regard to the use of company-approved removable data storage devices:

(a) Data security and integrity are maintained.

(b) Risks to the stability of company IT systems and networks are kept to a minimum.

(c) The risk of exposing sensitive company data is minimized while the removable media is offsite.

3 SCOPE

3.01 This directive applies to all individuals who are authorized to use company computer systems.

4 RESPONSIBILITY

4.01 All users are responsible to follow company-supplied processes and procedures documented for removable media to protect company data, IT systems and networks from the risks of using, transporting, reallocating and decommissioning these devices

4.02 IT Technical Support is responsible:

(a) To evaluate all removable media considered for company use and identify which of these are approved for acquisition and use on company IT systems.

(b) To identify which data encryption and password protection schemes are appropriate for protecting data on removable media while offsite.

(c) To effectively remove all data stored on removable media prior to reallocating or decommissioning the media.

(d) To evaluate system tools that control and/or log the attachment, removal and use of removable media.

4.03 IT Operations is responsible to monitor removable media connect/disconnect logs if these are implemented.

5 DEFINITIONS

5.01 "**Removable media**" includes all devices and data media that can have data written to them and subsequently be removed easily from the host computer, thus conferring portability on the data therein. This applies to devices such as:

- Optical disks (CD/DVD and Blu-ray)
- Magneto-optical disk
- Tape cartridges
- Cartridge drives (Jaz, SuperDisk, and ZIP)
- Flash memory devices (USB "sticks") and SD cards and similar devices
- USB-attachable data devices, including:
  - Hard drives
  - Digital audio and video players (iPod, MP3)
  - Digital cameras
  - Smart phones and other cellular phones
  - Handheld PCs and Personal Digital Assistants (PDAs)
  - Digital picture frames

6 RELATED DIRECTIVES

OCIO IT 8.02 – Systems Security

OCIO IT 8.04 – Confidentiality and Privacy

OCIO IT 9.02 – Data Classification

OCIO IT 9.03 – Data Access Controls

OCIO IT 9.04 – Application Security Controls

OCIO IT 9.06 – Data Encryption

OCIO IT 13.01 – System Access and Acceptable Use

OCIO IT 13.03 – Passwords

OCIO IT 14.01 – BYOD: Acceptable Devices and Operating Systems

OCIO IT 14.02 – BYOD: System Access and Acceptable Use