Removable Storage Media

313.1 PURPOSE:
To establish guidelines regarding the use of physically removable storage media, including Universal Serial Bus (USB) or any plug in devices, throughout the Department.

Information contained on such devices can be easily compromised if the device does not have adequate protective features.In addition, removable storage media (RSM), such as USB thumb drives, MP3 players, Optical Media (CD-R, CD-RW, and DVD's) floppy disks, external hard drives, memory cards (CF, SD, etc.), and wireless cards that have mass storage capacity can create risks to the County's network and data.Due to these risks, their use must be monitored.

313.2 DEFINITIONS:
Flash Drive: A USB or similar type 2 or 3 plug in flash drive is flash memory integrated with a USB or similar port.It is a small, lightweight removable data storage device.This hot swappable, solid-state device, is usually compatible with systems that support the USB version that the drive uses.

Digital Music Player: A portable consumer electronic device that allows storage and reproduction of music files in digital/audio format.These USB compatible devices also allow the storage and retrieval of other file types and can act as external hard drives.

Optical Media: An optical storage disc for digital data.CDs and DVDs have different read/write capabilities and are read or written to by an optical drive.

Floppy Disks: Magnetic storage read or written to by a floppy disk drive.This type of media is becoming increasingly obsolete and common sizes are 5.25" and 3.5", with different storage sizes based on the size of the disk.

External Hard Drives: A type of hard disk that is externally connected to a computer via an external port.

Memory Cards: An electronic memory data storage device used with digital cameras, handheld and mobile computers, telephones, music players, video game consoles, and other electronic devices.These memory cards offer high re-record ability, power free storage and can be connected to a USB port with a card reader.

Wireless Cards: An external port card with an external port that resembles a flash drive and is used for wireless laptops in conjunction with Virtual Private Networking (VPN) software to facilitate staff access to internal department resources.These devices can employ an external port for Removable Storage Media to allow for the use of a memory card.These devices are not to be used for storage of any department information (confidential or non-confidential).

Digital Voice Recorder: A small hand-held device used to convert speech and other sounds into digital files. These files can then be transferred to other electronic devices such as a computer, tablet, or smartphone for storage.

Smartphones (Android, IOS): A cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, internet access, and an operating system capable of running downloaded applications. Smartphones can browse the Internet and run software programs like a computer in addition to calls and text messages.

Confidential Information: Electronic data including, but not limited to, information in any amount about probationers, casework, cases, criminal or gang intelligence, data preserved for evidentiary or investigative purposes, Training Unit PowerPoint Presentations, or personnel information.Data constituting public record information that is accessible only by subpoena shall be treated as confidential information.

Non-Confidential Information: General data whose acquisition would not benefit an outside entity, which may include but is not limited to public record information, financial information such as budgets without account numbers or employee identifiers, recruiting material, program overviews, and policy or procedure information.

Short Term Use: A special project, assignment, or other use for less than three (3) months (Obtain most current form from Automated Services).

Long term Use: Any use over three (3) months (Obtain most current form from Automated Services).

313.3 RESPONSIBILITIES:

I. All Staff:

A. Shall use only department approved RSMs issued by the Automated Services Unit to hold or transfer department data, except as described in the Guidelines section of this procedure.RSMs will be issued on a case-by-case basis based on position assignment and similar parameters, and if approved, may take up to two (2) business days to process after receipt of the request by Automated Services.Only business-related items may be stored on a RSM.If used to transfer data, the data shall be transferred from one department owned or approved computer to another department owned or approved computer.

B. When a department employee has determined that a media device has exceeded its useful life, and/or the employee is transferring to another position, and/or an employee is separated from employment, shall submit the device to Automated Services for processing.Department personnel returning media devices to Automated Services after use must ensure that the data contained on it has been copied elsewhere or is no longer needed.

C. Employees requesting use of RSMs due to their current assignment shall request a RSM Checkout Form from Automated Services and submit it to their supervisor.

D. Shall immediately report to their Supervisor if a department-issued media device is lost or stolen.

E. Shall provide the RSM to Management, Administration, and/or Automated Services staff upon request.

II. Supervisors:

A. Review RSM Checkout Form submitted by staff.

B. Forward RSM request to respective Division Director for approval when appropriate.

III. Automated Services:

A. Upon Division Director approval, shall issue the requested RSM to the employee.

B. Upon receipt of a RSM, shall determine whether the device is re-usable or should be destroyed.

C. Shall perform a Secure Deletion of the device by purging all data through use of approved deletion software or devices and/or ensure destruction.

D. Shall conduct random reviews of RSMs.

E. Shall be responsible for providing temporarily assigned RSMs as specified by Directors/Administration with the appropriate number for each area determined by Directors/Administration.

F. In order to ensure proper support functions of department hardware, software, and infrastructure needs, shall maintain Administrative rights on all department systems in regards to the use of RSMs.

G. Shall be responsible for the issuance, destruction, and maintaining documentation on all issued and returned RSM.

H. Shall make the following methods of data transfer available:

1. Request for a large volume of data storage, particularly when that data is specialized or germane only to that unit; may create a separate directory folder on the department's shared storage space.

2. Personnel requests requiring archived preservation of data, storage of a large volume of data, or transfer of a large volume of data between employees or units; may download the data to an appropriate RSM.This RSM shall be provided to the employee.

3. Any request described in 1-2 above shall be made via an "ITD Help Desk ticket" request, following approval by their respective Division Director.

IV. Division Directors:

A. Shall be responsible for approving all requests for RSMs (long term and short-term assignment).For short-term assignment, the completed form shall specify the project and approved time period.

B. Review RSM requests and upon approval shall forward the request to Automated Services for the issuance of an RSM.

C. Shall be responsible for the control, collection, and documentation of all RSMs issued and will be responsible for ensuring RSMs are provided to Automated Services staff for the inspection process and as determined by management.

313.4 GUIDELINES:

A. Data on disaster recovery, crisis response, multi-agency operational planning, NIMS planning, criminal intelligence, training or other information to be shared or exchanged between agencies may be transferred using any department-issued RSM, providing the RSM is securely transported and controlled at all times while in the possession of department staff.It is recognized that information is commonly shared between agencies, particularly during operations and training.

B. RSMs are a useful method for the short-term storage or transfer of data between personnel, units, assignments, etc.

C. RSMs issued by Automated Services are County property and are subject to inspection, retrieval and review of all data at any time.

D. Confidential information shall only be sent using County e-mail/webmail, and may only be sent to recipients outside the County email system using encryption as defined in the Electronic Communications Procedure.