# FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

**Title:** Mobile Devices Procedures

**Related Policy:** FDJJ – 1230

## I. DEFINITIONS

**Agency-Owned Device –** A Mobile Device (as defined in this document), owned by the agency and used to conduct agency business or perform agency duties. The agency develops standards and policies to govern the usage of the device which are disseminated to the user to ensure compliance.

**Agency-Managed Device –** A Mobile Device (as defined in this document), owned by a consultant, contractor, or provider and used to perform agency duties or conduct agency business. Usage of these devices must be approved by the applicable Executive Leadership member and the agency's CIO prior to use. The device owner shall allow the Department to manage the device and abide by the agency's standards and policies governing usage of the device.

**Anti-Malware Software –** Software installed on a computing device protecting it from malicious software.

**Authenticated User –** An authorized agency employee using the Department of Juvenile Justice's information technology resources, who has completed the "Authentication" process as defined below.

**Authentication –** The process of verifying a user is who he or she claims to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or the iris of the eye.

**Availability –** Authorized users have access to information and assets.

**Bluetooth –** Bluetooth is a telecommunications industry standard that allows mobile devices, computers, and other devices to easily communicate with each other using a short-range wireless connection.

**Bureau of Information Technology (IT) Personnel –** Individuals who maintain or administer information technology resources on behalf of information owners. The person or team who holds the day-to-day responsibility for information technology infrastructure resources.

**Chief Information Officer (CIO) –** DJJ staff responsible for overseeing the Bureau of Information Technology (IT) within DJJ.

**Confidential Information and/or Confidential Data –** Information/Data exempted from disclosure requirements under the provisions of applicable state and federal laws.

**Confidentiality –** Information is accessible only to those authorized.

**Contract/Grant Manager –** DJJ staff responsible for management of contracts and grants within a DJJ branch.

**Copy of Record –** The official copy of a document, spreadsheet, PowerPoint presentation, etc. retained by the agency until the official retention period has been met.

**Data Integrity Officer (DIO) –** DJJ staff responsible for assisting users with maintaining the integrity of the data entered in the Juvenile Justice Information System (JJIS), creating JJIS user accounts, and assisting with JJIS training.

**Department of Juvenile Justice (DJJ) –** Hereinafter known as the agency.

**Direct Connect [to the agency network] –** A mobile device that is joined to and becomes an extension of the agency's internal network, i.e. Internet Access, Citrix/UAS access, or dialup access.

**Encryption –** The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Advanced Encryption Standard (AES) 256-bit encryption algorithm is the DJJ standard.

**Firewall –** Software installed on a computer or device which helps protect that system against unauthorized access.

**Information Owner –** The executive business manager who is responsible for the collection, maintenance, and dissemination of information; the person who creates or initiates the creation or storage of information; and/or the person or group responsible for applying security policies to an information object.

**Information Security Manager (ISM) –** The person designated to administer the agency's information resource security program and plans in accordance with Section 282.318(2)(a)1, F.S., who acts as the agency's internal and external point of contact for all information security matters.

**Information Technology Resources –** Agency computer hardware, software, networks, devices, connections, applications, and data.

**Integrity –** Assurance that data/information remains intact, correct, and authentic. Protecting the integrity involves preventing unauthorized creation, modification, disclosure, or destruction of data/information.

**Mobile Computing Device –** A laptop, PDA, or other portable device that can process data.

**Mobile Devices –** General term describing both mobile-computing and mobile-storage devices.

**Mobile Storage Device –** Portable data-storage media including, but not limited to, external hard drives, memory cards, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital video discs (DVD-R/RW), IPOD, media players, cell phones, or tape drives that may be easily attached to and detached from computing devices.

**Owner of an Information Technology Resource –** The manager of the business unit ultimately responsible for the information resource.

**Pairing –** A process used in computer networking that helps configure an initial connection between computing devices to allow communications between them. The most common example is used in Bluetooth, where the pairing process is used to link devices like a Bluetooth headset with a mobile phone.

**Property Coordinator –** Staff members from each regional program area responsible for property functions.

**Property Custodian –** DJJ staff who receives authority to manage property from either a property coordinator, property liaison, or other supervisory staff.

**Property Liaison –** Staff member in each facility or administrative office responsible for property functions.

**Provider –** Any non-DJJ entity providing a juvenile service for the agency.

**Provider Director –** The person, within the provider's management organization, who is responsible for compliance with DJJ contract requirements.

**Recipient –** Any authorized staff member who has been assigned an agency-owned mobile computing and/or mobile storage device to complete work-related responsibilities.

**Remote Access –** Any access to the agency's corporate network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carrier, or other external connectivity).

**Supervisor –** Responsible for ensuring their employees understand and comply with agency policies and procedures.

**Text Messaging/Texting –** The act of composing and sending electronic messages, typically consisting of alphabetic and numeric characters, between two or more users of mobile phones, fixed devices (e.g., desktop computers) or portable devices (e.g., tablet computers or smartphones).

**User –** Any authorized person who uses the Department of Juvenile Justice's information technology resources, including providers and temporary users.

## II. STANDARDS/PROCEDURES

A. Mobile Devices – General Requirements:

1. All security and privacy policies applicable to users of computing resources within an agency facility shall apply when using or connecting to agency information technology resources from outside the agency facility. Reference the Related References section of the Mobile Devices Policy.

2. The Bureau of Information Technology has sole discretion for approving authorized remote access to DJJ's network, including the standard remote access software utilized for access.

3. Only agency-owned or agency-managed mobile storage devices shall be used to store agency data.

4. All agency-owned mobile computing devices shall be approved by the Department of Juvenile Justice's Bureau of Information Technology (IT) via the Information Resource Request (IRR) process prior to purchase.

5. Mobile-computing devices connecting to DJJ's network shall use agency-approved up-to-date anti-malware software.

6. Department issued laptops shall be directly connected to the Department's network at least once every thirty (30) days to ensure the device is encrypted and has the latest operating system, software, and malware prevention updates.

7. Agency-owned mobile devices shall be configured and maintained according to agency standards.

8. Only agency-approved software shall be installed on agency-owned or agency-managed mobile computing devices.

9. Agency-owned mobile computing devices shall only be issued to and used by authenticated users.

10. Personally-owned devices shall not be used to store agency data.

11. Only agency-owned or agency-managed mobile storage devices may store agency data.

12. All agency-owned and agency-managed mobile computing devices shall be secured with a password-protected screensaver set to automatically activate after 15 minutes (or less) of inactivity where technology permits.

13. All agency-owned/managed mobile storage devices shall use encryption technology to ensure the data (i.e. documents, files, records, etc.) stored on the device is stored in an encrypted state.

14. All agency-owned/managed mobile devices must be encrypted with 256-bit AES encryption. This includes, but is not limited to, mobile-computing devices and mobile-storage devices.

15. Confidential information shall be accessible only to authorized individuals.

16. Users must take reasonable precautions to protect confidential information in their possession from loss, theft, tampering, unauthorized access/disclosure, and damage.

17. Users must take reasonable precautions to protect mobile-computing and mobile-storage devices in their possession from loss, theft, tampering, unauthorized access, and damage.

18. To prevent loss of agency data stored on mobile devices, devices shall be backed up at an agency approved location and stored in an agency approved format.

19. Agency data, stored on mobile-storage devices that do not have encryption technology (i.e. format floppy disks, recordable compact discs, and recordable digital video discs), shall be saved in a file or folder that has been encrypted.

20. If agency data is stored on an unencrypted device, the user must remove the data from the device immediately or contact their local Bureau of Information Technology representative to have the device encrypted immediately.

21. Confidential data shall be encrypted when transmitted over a network.

22. Users shall report the theft or loss of mobile or storage devices to the appropriate supervisor, DJJ ISM, and the Central Communications Center (CCC) within twenty-four (24) hours.

23. All agency-owned/managed mobile storage devices shall have encryption technology enabled such that all content resides encrypted, where technology permits.

24. Records shall not be stored solely on mobile-storage or mobile-computing devices. Mobile-storage devices shall only be used to store copies of data (i.e. documents, files, records, etc.) that have been stored elsewhere on a non-mobile device.

25. Data (documents, files, and records, etc.) saved on mobile-storage devices shall not be the official document or copy of record.

26. Use of Bluetooth technology on agency smartphones shall be limited to pairing with Bluetooth headsets and pairing to vehicles with Bluetooth capability. The use of Bluetooth technology on agency smartphones shall **NOT** be used for internet access by tethering to laptops or desktops. Additionally, the use of Bluetooth technology on agency smartphones shall **NOT** be used for the data transfer of files between smartphones and laptops, desktops, or other connected devices.

27. DJJ-owned mobile devices shall only be issued to authorized users in order to assist in conducting State of Florida business. Limited, non-commercial personal use of the internet access on a DJJ-owned mobile device shall be permitted only during non-work/unpaid hours as stated in FDJJ 1205.40 Internet Access and Use Policy.

B. Thumb/Jump Drives:

1. All agency-owned or agency-managed thumb/jump drives shall be encrypted. DJJ currently employs technology encrypting thumb/jump drives if they are used on a DJJ computer. Contact your local Bureau of Information Technology representative for additional information.

C. Mobile Devices:

1. All agency-owned or agency-managed mobile-computing and mobile-storage devices shall have encryption technology enabled such that all content resides encrypted, where technology permits.

D. Mobile Storage Devices:

1. Encryption technology shall be used on all agency-owned or agency-managed mobile storage devices to ensure the data (i.e. documents, files, records, etc.) on the device is stored in an encrypted state.

2. The 256-bit AES encryption shall be the agency standard for data (i.e. documents, files, records, etc.) and mobile-computing and mobile-storage devices.

E. Enforcement:

1. Any user of the Department of Juvenile Justice Information Technology Resources found to have violated this policy may be subject to disciplinary action up to and including termination of employment and/or criminal prosecution.

F. Exemption:

1. The Department's General Counsels shall be exempt from the encryption requirement while representing DJJ during legal proceedings in a court of law. Members of the Department's General Counsel staff understand the risks associated with confidential data, and therefore assume responsibility for unencrypted confidential data in their possession while working on behalf of the Department.

## III. RESPONSIBILITY AND DUTIES

The Bureau of Information Technology (IT) and the Bureau of General Services shall provide guidance for *and* jointly manage the procurement, operation, and surplus of office machines with data storage capability.

A. Contract/Grant Managers:

1. Responsible for ensuring the Provider Director is knowledgeable of and understands this and related policies as identified in the "Related References" section of this policy affecting applicable service providers.

2. Responsible for conveying to the appropriate Provider Director any revisions to this policy or current policies as identified in the "Related References" section of this policy affecting applicable service providers.

B. Data Integrity Officer (DIO):

1. Responsible for ensuring providers have read and understand this and related policies as identified in the "Related References" section of this document prior to establishing JJIS access.

2. Responsible for reporting the theft or loss of confidential agency data and/or mobile-computing/mobile-storage devices containing confidential data to the agency's ISM and the CCC immediately after learning about such loss or theft.

C. Information Owners:

1. Responsible for ensuring any mobile-computing resources are being managed and used in accordance with the procedures and guidelines set forth in this policy.

2. Responsible for ensuring any remote access to their information resources is conducted in accordance with the procedures and guidelines set forth in this policy.

D. Information Security Manager (ISM):

1. Responsible for auditing the use of mobile-computing devices to ensure compliance with the procedures and guidelines set forth in this policy and defining security countermeasures that will be applied.

2. Will report the loss or theft of mobile devices to applicable internal offices within the agency and other state agencies when necessary after receiving notification from users.

E. Bureau of Information Technology (IT) Personnel:

1. Applicable Bureau of Information Technology personnel shall inspect all office machines with data storage capability during the disposition and disposal process to ensure the removal of all data-storage media (i.e. hard drives, flash drives, USB devices, optical disks, memory, etc.) from the device and securely sanitized ***before*** the device/media leaves DJJ facilities.
2. Applicable Bureau of Information Technology personnel shall complete the ***Data Storage Media Sanitization/Destruction Form*** (Form 1260-1) to document and verify the sanitization of all data-storage media (i.e. hard drives, flash drives, USB devices, optical disks, memory, etc.). If the device is being surplused a Surplus Certification of State Property (Form 25) must also be completed and attached to the form 1260-1.

F. Property Custodians/General Service Liaisons:

1. Responsible for providing secure storage for any such device in their custody.

2. Shall work with the Bureau of Information Technology to ensure only mobile computing and mobile storage devices with encryption capability are purchased on behalf of the agency.
3. Shall work with the Bureau of Information Technology to ensure all office machines with data storage capability are inspected by the applicable Bureau of Information Technology personnel during the disposition and disposal process to ensure all data-storage media (i.e. hard drives, flash drives, USB devices, optical disks, memory, etc.) is removed from the device and securely sanitized *before* the device/media leaves DJJ facilities.
4. Shall work with the Bureau of Information Technology to ensure proper documentation (such as forms 25 and 1260-1 are completed in order to document and verify the sanitization of all data-storage media).

G. Providers:

1. Responsible for complying with the procedures and guidelines set forth in this policy and observing the agency policies and procedures as identified in the "Related References" section of this policy.

2. Shall not save or store agency data on any unencrypted mobile computing or storage devices.

3. Responsible for using all due diligence to protect the agency's data when handling, sharing, maintaining, storing and/or transporting agency data.

4. The Provider Director or designee at each provider facility shall be responsible for reporting the theft or loss of mobile computing or storage devices to the appropriate supervisor and their DJJ Contract/Grant Manager or DIO by E-mail or telephone within twenty-four (24) hours of learning about such loss or theft.

5. The Provider Director or designee at each provider facility shall be responsible for immediately filing a police report detailing the theft or loss of any agency data, mobile computing, and mobile storage devices.

6. The Provider Director or designee at each provider facility shall be responsible for submitting police reports and cooperating with applicable agency staff (i.e. DIOs, Contract/Grant Managers, ISM, and Inspector General) in collecting information pertaining to the theft or loss of agency data and/or mobile computing/storage devices.

7. The Provider Director or designee at each provider facility shall act as the Property Custodian as outlined in Section III. E. of the policy procedures.

H. Supervisors:

1. Responsible for ensuring their employees understand and comply with this and related policies as identified in the "Related References" section of this policy.

2. Responsible for ensuring employees under their supervision report the loss or theft of any mobile computing/storage device to the Department's ISM and CCC immediately after learning about such loss or theft.

3. Responsible for ensuring employees under their supervision report the loss or theft of any agency data to the Department's ISM and CCC immediately after learning about such loss or theft.

4. Responsible for ensuring employees under their supervision adhere to agency policy regarding texting and report any misuse of agency devices for purposes other than intended.

5. Shall cooperate and ensure employees under their supervision cooperate with applicable agency staff (i.e. DIOs, Contract/Grant Managers, ISM, and Inspector General) in collecting information pertaining to the theft or loss of agency data and/or mobile computing/storage devices.

6. Shall, under the direction of their ELT member, file a police report detailing the theft or loss of any agency data, mobile computing, and mobile storage devices that occur under their direct supervision.

7. Shall work with the Bureau of Information Technology to ensure only mobile computing and mobile storage devices with encryption capability are purchased on behalf of the agency.

I. Users:

1. Responsible for complying with the procedures and guidelines set forth in this policy and observing the agency policies and procedures identified in the "Related References" section of this policy.

2. Will not save or store any agency data on any unencrypted mobile-computing or mobile-storage device.

3. Responsible for using all due diligence to protect the agency's data and mobile-computing/storage devices when handling, sharing, maintaining, storing, and/or transporting information.

4. Responsible for reporting the theft or loss of any agency data to their supervisor, DJJ ISM, and CCC within twenty-four (24) hours of learning about such loss or theft.

5. Responsible for reporting the theft or loss of mobile or storage devices to their supervisor and DJJ's ISM within twenty-four (24) hours of learning about such loss or theft.

6. Responsible for scheduling maintenance (via the Bureau of Information Technology Work Order) for Department-issued mobile devices when notified to do so by Information Technology personnel.

7. Shall directly connect the Department issued laptops in their possession to the Department's network at least once every thirty (30) days to ensure the device is encrypted and has the latest operating system, software, and malware prevention updates.

## IV ATTACHMENTS

Attachment 1 - AD-IS 1230-1 Encrypted Mobile Device Acknowledgement.

Attachment 2 - AD-IS 1230-2 Mobile Devices Property Custody Log

Related Policy/Form: FDJJ 1260 Security Requirements for Office Machines with Data Storage Capability

AD-IS 1260-1 Data Storage Media Sanitization/Destruction Form