FLORIDA DEPARTMENT OF JUVENILE JUSTICE POLICY

Secretary /s/, Simone Marstiller **Date:** 8/26/2019

Subject: Mobile Devices Policy

Section: FDJJ – 1230

Originating Office: Administrative Services

Authority: F.S. Chapters 119, 282, 984 and 985

Related References: Florida Administrative Code, Rule 71A-1
Sections 282.318 and 119.07, Florida Statutes;
FDJJ Policy 1316, Records and Information Management
FDJJ Policy 1312, Property Management and Control
FDJJ Policy 1205.20, Computer Malware Protection;
FDJJ Policy 1205.30, Information Resource Security Standards & Guidelines;
FDJJ Policy 1205.60, Provider Access to Juvenile Justice Information System (JJIS) and JJIS Data

Purpose: This policy provides guidelines for mitigating the security risks posed from the use of mobile computing and mobile storage devices.

Offices Affected by the Policy: All offices within the Department of Juvenile Justice (DJJ) and applicable service providers/consultants.

POLICY STATEMENT:

- All DJJ staff, providers, vendors, and third parties using DJJ's Information Technology Resources and/or accessing DJJ data, shall adhere to this policy.
- 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.
- Only agency-owned or agency-managed mobile storage devices may store agency data.
- Only agency-approved software shall be installed on agency owned or agency managed mobile computing devices.
- Personally-owned devices shall not be used to store agency data.
- All agency-owned and agency-managed mobile computing devices shall be secured with a password-protected screensaver which is set to automatically activate after 15 minutes (or less) of non-activity, where technology permits.

- Users shall take reasonable precautions to protect both the agency's computing and storage devices and any agency data in their possession from loss, theft, tampering, unauthorized access/disclosure, and damage.
- All agency-owned and agency-managed mobile computing and mobile storage devices shall have encryption technology enabled such that all content resides encrypted.
- Users with text-activated devices shall take reasonable precautions to protect agency data transmitted on such devices. Such users shall not use these devices in their possession for personal texting.
- 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.
- All office machines with data-storage media shall be inspected by the Bureau of Information Technology (IT) 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 is removed from a DJJ facility.
- The *Data-Storage Media Sanitization/Destruction Form* (Form 1260-1) shall be completed 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.
- Users shall report the theft or loss of mobile or storage devices to the appropriate supervisor, DJJ's Information Security Manager, and the Central Communications Center (CCC) within twenty-four (24) hours.
- Users shall consult their local Bureau of Information Technology representative for guidance on encrypting agency data and/or mobile devices.
- 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.

PROCEDURES/MANUALS:

Procedures for this policy are accessible at the Department Policies internet page.