FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Security Requirements for Physical and Electronic Media

Related Policy: FDJJ - 1260

I. DEFINITIONS

Data Storage Media – Refers to material used to electronically record and/or store data and images, such as hard drives, flash drives, thumb/jump drives, magnetic tape, magnetic disks, optical disks, and solid-state devices. **Note**: The term "media" shall be used throughout this document to refer to data storage media.

Degaussing – The process of exposing magnetic data storage or media to a strong magnetic field in order to disrupt (erase) the recorded magnetic domains.

Encryption – Transforming readable text into unreadable text (cipher) for the purpose of security. Advanced Encryption Standard (AES) 256-bit encryption algorithm is the DJJ standard.

Information Resource Request (IRR) – A standard form used within DJJ for requesting approval from the Chief of Information Technology (IT) to acquire information technology resources.

Media Sanitization – Actions taken to render stored data and/or images unrecoverable by both ordinary and extraordinary means. The most common types of sanitization are destruction (*e.g.*, burning, shredding, or disintegrating), degaussing (*i.e.*, demagnetizing), and overwriting. **Note**: The terms "sanitization," and "sanitize" shall be used interchangeably throughout this document to reference media sanitization.

Multi-Function Devices (MFD) – Office machines which incorporate the functionality of multiple devices into a single device. MFDs are also referred to as Multi-Function Printer/Product/Peripheral (MFP) or all-in-one (AIO) devices. MFDs referenced in this policy have the ability to store data and/or images of documents copied, scanned, faxed, or e-mailed from them. **Note**: The term "device" shall be used throughout this document to refer to office machines with data storage capability.

Non-Volatile Memory – Memory which saves data and images when the computer or device is shut down. Examples are hard drives, memory cards, jump/thumb drives, etc.

Overwrite – A process for secure destruction of data without rendering the hard drive useless. Overwriting replaces existing data on a hard drive with meaningless data in such a way, the original data cannot be recovered.

Password Hard Drive Lock – A feature available in many MFDs which locks the device's hard drive using an alphanumeric password.

Physical Destruction – Damaging the medium so it is unusable in a computer and no data can be retrieved.

Security Overwrite – A feature available in many MFDs which erases the data stored on the device's hard disk drive or memory by pressing a series of characters/keys.

II. STANDARDS/PROCEDURES

A. Procuring/Leasing Office Machines with Data Storage Capability:

1. All applicable office machines using hard drives for data storage shall be procured with removable hard drives that will be owned/retained by the Department when the device has to leave the facility for repairs or at end-of-life/end-of-lease.

2. All applicable office machines with non-hard drive data storage media (i.e. flash drives, thumb/jump drives, optical disks, etc.) shall be procured with an option for the Department to own/retain the media when the device has to leave the facility for repairs or at end-of-life/end-of-lease. All office machines with data storage media, regardless of price, shall be reviewed, approved by the CIO prior to procurement and /or connection to the DJJ network.

3. An Information Resource Request (IRR) shall be submitted to the local IT Regional Leader and the CIO for the purchase/lease of all office machines with data storage media, regardless of cost.

4. All renewal, lease, and/or purchase requisitions (PR) for office machines with the ability to store data and images must be accompanied by a previously approved IRR.

5. Reference FDJJ 1675, Section II, F, #7 and 15 for additional details regarding IT Goods and Services and Rental and Leasing equipment.

6. Office machines with hard drive data storage media shall be purchased with the Disk Encryption option/function (where technology permits)—**reference Section II, C. Disk Encryption and Image Overwrite, for details**.

7. All applicable office machines with data storage media shall be purchased with Image Overwrite option/function (where technology permits)—**reference Section II, C. Disk Encryption and Image Overwrite, for details**.

B. Renewal Agreements:

1. Renewal Agreements for office machines with non-volatile data storage media must, if not written in previous agreements, be written to include an option allowing the Department to own/retain the data storage media when the device has to leave the facility for repairs or at end-of-life/end-of-lease.

2. Renewal Agreements for office machines with non-volatile data storage must, if not written in previous agreements, be written to include the Disk Encryption option/function (where technology permits).

3. Renewal Agreements for office machines with non-volatile data storage must, if not written in previous agreements, be written to include the Image Overwrite option/function (where technology permits).

C. Disk Encryption and Image Overwrite:

Disk Encryption and Image Overwrite shall be enabled on all office machines with data storage capability where technology permits.

1. Disk Encryption – Enable this feature to use 256-bit AES encryption to secure data.
2. Image Overwrite – Enable this feature to remove all image/data from the hard drive and other forms of non-volatile storage. This feature shall be set to **Immediate Overwrite**.
3. Immediate Overwrite – Jobs automatically overwritten immediately after the job is completed.

D. Sanitization of Data Storage Media:

1. The data storage media (i.e. hard drives, memory cards/sticks) of all applicable MFDs shall be sanitized so there is reasonable assurance the data may not be retrieved and reconstructed.
2. The data storage media of all applicable MFDs shall be reimaged before the media or the device itself is reassigned to another section, bureau, or program office within the Department to prevent unauthorized access to the Department's data. **Note**: Data storage media shall only be re-used/reassigned within the Department. It shall not be surplused.
3. Office machines with multiple forms of data storage media storage may require multiple methods of sanitization. For example, sanitizing a network printer with a hard drive and RAM requires the device be powered off/on and reset to factory standards to sanitize the RAM along with a hard drive reformat to sanitize all data from the hard drive.
4. Acceptable methods of media sanitization include software overwrite, degaussing, reformatting, or physically destroying media. **Note:** File deletion is not an acceptable method of sanitization.
5. The sanitization method used shall be documented on the Data Storage Media Sanitization/ Destruction Form (Attachment 1).

E. Configuration of Office Machines with Data Storage Capability:

1. All Department-owned or leased office machines with data storage media shall be configured to operate in compliance with all applicable IT policies.
2. All Department-owned or leased office machines with data storage media with an underlying MS Windows™ based operating system must receive regular (hardware and software) maintenance.
3. All Department-owned or leased office machines with data storage media shall be configured to allow e-mail to internal/DJJ e-mail addresses only.
4. The ability to send faxes shall be allowed on all Department-owned or leased office machines with data storage capability provided fax functionality is transmitted over a traditional telephone landline.

5. The Cloud-Computing (i.e. Scan-to-Web) feature shall be disabled on all applicable Department-owned or leased office machines with data storage capability.

6. A Data Storage Media Configuration Checklist (Attachment 2) shall be completed by the installer to document the device information and configuration settings on all applicable devices during the initial setup.

F. Network Configuration of Office Machines with Data Storage Capability:

1. Department-owned or leased office machines with data storage media shall not be attached to the DJJ network without the prior authorization from the Department's CIO in the form of an approved IRR.

2. Department-owned or leased office machines with data storage media shall be isolated on the local area network. A firewall shall be used to block all ingress and egress traffic from the MFD.

3. Each Department-owned or leased office machine with data storage media shall have an assigned static IP address so that if the Domain Name System (DNS) cache is corrupted, print files containing sensitive data cannot be redirected, leading to the further compromise of sensitive data.

4. The default vendor password on all Department-owned or leased office machine with data storage media shall be changed to a password meeting the Department's "strong" password standards (e.g. eight or more alphanumeric characters and punctuation marks, combining UPPER and lowercase letters).

G. Prohibited Practices for Office Machines with Data Storage Capability:

1. Department-owned or leased office machines with data storage media regardless of cost shall not be connected to the Department's network without prior approval from the Department's CIO in the form of an approved IRR.

2. Office machines with data storage media shall not be used on behalf of the Department if the device cannot be operated in compliance with all applicable IT and General Services policies and procedures **(see Related References)**.

3. Sending/Transmitting group faxes from Department-owned or leased office machines with data storage media shall be allowed provided fax functionality is transmitted over a traditional telephone landline.

4. Data storage media shall only be re-used/reassigned within the Department. It shall not be surplused for use outside of the Department.

H. Destruction of Electronic and Physical Media:

1. DJJ Staff will contact the vendor and schedule the onsite media destruction.
2. Prior to the destruction date, DJJ staff will prepare a DJJ Storage Media Disposition Log listing all storage media devices to be destroyed by the vendor.
3. At the time of destruction, the Vendor and DJJ staff will verify the quantity of storage media devices (physical to log count) and the vendor will complete the top portion of the log (vendor name, quantity received, received by name, and received by signature).
4. The vendor signed log form will be returned to the DJJ staff.
5. Vendor will record the serial number for each device being destroyed.
6. On the day scheduled, vendor will destroy the storage media onsite with a member of the Information Technology staff as a witness.
7. Within ten (10) business days of pickup, the Vendor will mail the certificate of destruction for all devices in the pickup lot to the following:

   Department of Juvenile Justice
   Information Technology
   Attention: IT Inventory Control
   2737 Centerview Dr., Suite 1400
   Tallahassee, FL 32399-3100

   Department of Juvenile Justice
   Information Technology
   Attention: Information Security Manager (ISM)
   2737 Centerview Dr., Suite 3300
   Tallahassee, FL 32399-3100
8. Internally, DJJ will distribute the Certificate of Destruction to the appropriate DJJ staff for validation against their DJJ Storage Media Disposition Log(s).
9. If there are any discrepancies, they will be reported to the DJJ ISM (Information Security Manager), who will coordinate contact with the vendor for any needed clarification and will document the results.

I. Exceptions:

1. Any exceptions to the aforementioned standards/procedures must be pre-approved by the Department's Chief Information Officer/Chief of Information Technology.

III. RESPONSIBILITY AND DUTIES

A. Department Head:

1. Shall ensure staff members read this policy prior to using DJJ information resources.

B. Chief Information Officer:

1. Shall review and approve acceptable IRRs from IT Regional Leaders.
2. Shall ensure IT personnel adhere to the guidelines established in this and other Department policies, procedures, and standards using tools and techniques to protect the integrity of the Department's data and technological infrastructure.

C. Purchasing Department - Purchasing Specialist:

1. Shall work with all DJJ program areas to ensure compliance of this policy as it relates to the procurement and surplus of office machines with data storage media.
2. Shall work with applicable manufactures/resellers and DJJ IT staff to ensure DJJ owned/leased devices have and utilize mechanisms to prevent unauthorized access to the data stored on the devices.

D. Information Technology (IT) Regional Leaders and Desktop Support Personnel:

1. Shall work with applicable manufactures/resellers and DJJ General Services staff to ensure DJJ owned/leased devices have and utilize mechanisms to prevent unauthorized access to the data stored on the devices.
2. IT Regional Leaders shall ensure applicable devices are configured based on the guidelines and recommendations established in this policy by reviewing IRRs and forwarding acceptable IRRs to the CIO—**reference Section II, F. Network Configuration of Office Machines with Data Storage Capability, for details**.
3. Shall, with the assistance of the Network Administrator, ensure the Department's network is configured based on the guidelines and recommendations established in this policy—**reference Sections II, F. Network Configuration of Office Machines with Data Storage Capability and E**. **Configuration of Office Machines with Data Storage Capability for details.**
4. Shall ensure applicable devices are sanitized or destroyed so there is reasonable assurance the data may not be easily retrieved and reconstructed—**reference Section II, D. Sanitization of Data Storage Media, for details**.
5. Shall ensure the data storage media (i.e. hard drive, flash drive, optical disk, memory, etc.) is removed from the device **before** the device is taken from DJJ facilities for repair or replacement/end-of-lease.
6. Shall ensure applicable data storage media has been securely sanitized and is only re-used in DJJ-owned/operated devices.

7. Shall ensure the default vendor password has been changed to a password meeting the Department's "strong" password standards (e.g. eight or more alphanumeric characters and punctuation marks, combining UPPER and lowercase letters).

E. DJJ Network Administrator:

1. Shall, with the assistance of the IT Regional Leaders and Desktop Support Personnel, ensure the Department's network is configured based on the guidelines and recommendations established in this policy—**reference Section II, F. Network Configuration of Office Machines with Data Storage Capability, for details**.

F. DJJ Managers:

1. Shall ensure the employees under their direct supervision are knowledgeable of and adhere to the guidelines established in this policy.

2. Shall submit a completed IRR to the applicable IT Regional Leader for the purchase, lease, and renewal (if applicable) of all office machines with data storage media, regardless of cost.

3. Shall ensure applicable devices purchased/leased under their direct supervision are placed in an access-restricted environment.

4. Shall ensure keys to applicable devices are placed in an access-restricted environment and are only accessible by authorized personnel.

5. Shall ensure the password to applicable devices are only divulged on a need-to-know basis.

6. Shall coordinate with local IT personnel (via the Department's IT Work Order System) to ensure data storage media is removed from devices falling under their supervision before the device is removed, surplused, or returned to vendors at lease end.

G. Department Employees and Other Applicable Users:

1. Shall comply with this policy and applicable local, state, and federal IT-related policies.

2. Shall report any known or suspected misuse of DJJ Information Technology resources to the Information Security Manager and/or the Chief of Information Technology immediately.

3. Shall take reasonable measures to ensure the confidential information he/she has access to is not subject to unauthorized disclosure or destruction. This includes but is not limited to the following:

   a. Ensure documents are sent to the correct printer before printing the document.

   b. Ensure documents containing confidential information are not left unattended on/in the devices.

IV. ATTACHMENTS

Attachment 1 - Data Storage Media Sanitization/Destruction Form

Attachment 2 - Data Storage Media Configuration Checklist