Section Name: Information Security Effective Date: April 2, 2019
Section Number: 800
Policy Number: 803

Subject: Media Sanitization and Destruction Policy

Purpose: The purpose of this policy is to outline the proper disposal/sanitization/destruction of media (physical or electronic) for Monroe County ("the County"). These rules are in place to protect sensitive and classified information, employees or contractors, and the County. Inappropriate disposal of Monroe County hardware and sensitive or other protected data may put the County at risk.

Scope: This policy applies to all employees, contractors, consultants, temporary staff, and other people or organizations who perform work for or at the County ("Users") with access to LEIN/CJIS/HIPAA/IRS 1075 or other sensitive, protected and classified data and media. This policy applies to all equipment that processes, stores, and/or transmits this information that is owned or operated on the Monroe County network.

Statement of Policy: When no longer usable, hard drives, flash drives, tape cartridges, DVDs/CDs, hard copies, print-outs and other similar items used to process, store and/or transmit classified and sensitive data shall be properly disposed of in accordance with measures established by the County.

A. Physical media (print-outs and other physical media) shall be disposed of (rendered incapable of reconstruction) by one of the following:
    1. Shredded using cross cut shredders
    2. Placed in locked shredding bins for disposal by the company contracted by the County to come on-site and cross-cut shred, witnessed by County personnel throughout the entire process
    3. Incineration using a qualified, company contracted by the County, and witnessed by County personnel onsite or at the incineration site, if conducted by non-authorized personnel

B. Electronic Media (hard drives, tape cartridge, CDs, flash drives, printer and copier hard drives, etc.) shall be disposed of by the Monroe County IT Department or person designated by the IT Director, using one of the following methods:

    1. Overwriting (at least three (3) times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. (i.e. Department of Defense (DOD) method)
    2. Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausser. Note that common magnets (e.g. those used to hang a picture on the wall) are fairly weak and cannot effectively degauss magnetic media.

3. Destruction - a method of physically destroying magnetic or optical media. As the name implies, destruction of magnetic or optical media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters or data bearing surfaces/components have been physically destroyed so that no data can be reconstructed.
4. Electronic media that is by its nature encrypted (certain smartphones, tablets, and Padlock drives), is self-encrypting (such as self-encrypted SATA hard drives), or capable of simultaneous universal erasure/factory reset (such as some solid state drives) may be sanitized by removing their encryption keys or issuing factory reset commands, but only if the documentation and actual use of the devices supports such sanitization. Otherwise, these devices must be sanitized by one of the methods named above.

C. Disposals shall be logged as appropriate to the data source.

D. Information Technology systems that have been used to process, store, or transmit sensitive or classified information shall not be released from the County's control until the equipment has been sanitized and all stored information has been cleared by the County IT Department.

Policy Compliance:

A. Responsibility- All Elected Officials/Judges/Department Heads, or their designee(s), are responsible for implementing the policies and procedures and ensuring staff and contractor compliance in their respective areas.

B. Compliance measurement - The IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits.

C. Exceptions- Any exceptions to the policy must be approved by the IT Department and Department Head or Elected Official for whom the User works.

D. Non-Compliance- An User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Definitions: None

Administrative Procedures: None

Legislative History of Authority for Creation or Revision:

Adopted pursuant to action of the Monroe County Board of Commissioners, dated April 2, 2019