



Policy: Electronic Data Destruction

ChildNet Number: CN 012.018
Original Approved Date: June 22, 2010
Policy Revised Date(s):
Policy Sunset Date:
COA Standard(s): RPM 6.02

Statement of Policy:

ChildNet's policy is to ensure that all electronic data is completely and securely destroyed according to Florida Statute(s).

Board Chair's Signature: _____

Date: _____

11/30/10



Procedure: Electronic Data Destruction

ChildNet Number: CN 012.018
Original Approved Date: June 22, 2010
Procedure Revised Date(s): June 10, 2014, February 14, 2024
Procedure Sunset Date:
COA Standard(s): RPM 6.02

Definitions

Hard Drive: a non-volatile storage device that stores digitally encoded data on rapidly rotating rigid platters with magnetic surfaces.

Optical Disc: a flat usually circular disc which encode binary data in the form of pits and lands on a special material on one of its flat surfaces.

Statement of Procedure

1. **Data Destruction Applicability:** This policy pertains to the destruction of all records and information created, received, or maintained by the agency on electronic media. This encompasses a wide array of media types, including:
 - a. Hard drives, both internal and external, where data is stored on magnetic platters.
 - b. Optical discs, such as CDs and DVDs, where data is encoded on physical surfaces.
 - c. Removable storage devices like flash drives and thumb drives.
 - d. Other electronic devices capable of storing data, including copiers and detachable hardware components.
2. **Destruction Methodology:**
 - a. All data residing on electronic storage media, be it digital (like SSDs), optical (such as CDs and DVDs), or traditional hard drives, will be subject to secure destruction processes.
 - b. The destruction of data and media will be conducted by a licensed and contracted vendor specializing in data destruction services. This ensures that the destruction process meets the required security standards and complies with relevant regulations and policies, including those outlined in DCF Media Protection (CFOP 50-28).



- c. Upon completion of the destruction process, the contracted vendor will provide certification to verify that the data and media have been securely and irreversibly destroyed, ensuring that recovery of any destroyed data is infeasible.

3. Vendor Selection and Oversight:

- a. Vendors will be selected based on their ability to meet stringent security standards for data destruction, including compliance with relevant state and federal regulations and industry best practices.
- b. ChildNet MIS department will maintain oversight of the destruction process to ensure compliance with this policy and the secure handling of sensitive information throughout the destruction lifecycle.

4. Documentation and Record-Keeping:

- a. Detailed records of all data destruction activities will be maintained, including the type of media destroyed, the date of destruction, the method used, and the certification of destruction provided by the vendor.
- b. These records will serve as an audit trail to ensure accountability and compliance with this policy and applicable regulatory requirements.

President's Signature: _____

Date: _____

04-02-24