I. PURPOSE

This policy ensures proper provisions are in place to protect information stored on media, both digital and non-digital, throughout the media's useful life until its sanitization or destruction. This policy identifies the family of controls for Media Protection (MP) as defined in NIST Special Publication 800-53 Rev 5.

II. DEFINITIONS

"Digital Media" - means portable, removable storage media or device used to store information. (ex. diskettes, magnetic tapes, desktops, laptops, hard drives, read only memory, compact disks, network equipment).

"Non-digital Media" - Hard copy or physical representation of information. (ex. paper copies, printouts, printer ribbons, drums, microfilm, platens).

III. POLICY

The controls outlined in the following sections detail the measures that should be implemented to protect information that is stored on media based on the classification of the information and regulatory requirements for Federal, State, and Agency. See Enterprise Standard 4080: Data Classification Standard for more information.

Marking**:** Media shall be marked in accordance with regulatory requirements.

Transporting**:** During transport, media shall be protected and controlled outside of secured areas and activities associated with transport of such media restricted to authorized personnel. Tracking methods shall be developed and deployed to ensure media reaches its intended destination. If sensitive information is transmitted via e-mail or other electronic means, it must be sent using approved encryption mechanisms. Please see Kentucky Information Technology Standard, for information concerning these requirements.

Storage: Media shall be physically controlled and securely stored in a manner that ensures that the media cannot be accessed by unauthorized individuals. This may require storing media in locked containers such as cabinets, drawers, rooms, or similar locations if unauthorized individuals have unescorted access to areas where sensitive information is stored.

Encryption: Information stored on digital media shall comply with regulatory requirements. See Kentucky Information Technology Standard, for enterprise standard requirements.

Retention: A media retention schedule shall be defined for all media in accordance with regulatory requirements. Agencies shall reference the KDLA State Government Records Retention Schedules.

Access Control**:** Only authorized individuals are permitted access to media containing State information. In addition to controlling physical access, user authentication will provide audit access information. Any access must also comply with any applicable regulatory requirements. Non-digital media should be hidden from the view of individuals that do not have authorization to access the information contained on or within the media.

The items outlined below are the responsibility of COT to sanitize or destroy media devices following the guidelines outlined below.

Asset	Description	Contains Data?	Sanitization Method (For Reused Assets)	Disposal Method (No Reuse Intended)
Server	Individual Servers, Rack Mount Servers, Desktop Servers	Yes	Secure Wipe	Secure Wipe and COT Shred
Hard Drive	Desktop Computer, Laptop, or Netbook	Yes	Secure Wipe	Secure Wipe and COT Shred
WAN Component	Router, switches, modems	Yes	Secure Wipe	Secure Wipe and COT Shred

The items outlined below are the responsibility of the agency to sanitize or destroy media devices following the guidelines outlined below.

Asset	Description	Contains Data?	Sanitization Method (For Reused Assets)	Disposal Method (No Reuse Intended)
Printer, Fax Machine, Copy Machine or Multi-Function Device	Network Printers, , Fax Machines, MFD	Yes	Secure Wipe	Secure Wipe and COT Shred
Phones, Pagers, Tablets	Cell Phone,, Smart Phone, GPS Phone, Tablet (IPad or Android Device), eReader	Yes	Secure Wipe	Secure Wipe and COT Shred
Removable Media	CD,DVD, USB Drive	Yes	n/a	COT Shred

Sanitization**:** Media must be sanitized in accordance with the requirements defined in NIST Special Publication (SP) 800-88 Rev 1, Guidelines for Media Sanitization (or its successor). Additionally, to ensure compliance with using approved devices, Agencies shall also consult the National Security Agency (NSA) Central Security Services' Media Destruction Guidance.

Certification of Sanitization**:** The sanitizing process shall be documented within ServiceNow with an Asset Disposal Request. This information must be maintained as outlined by the Kentucky Department of Library and Archives (KDLA) record retention schedule.

Sanitization of Portable, Removable Storage Devices Prior to First Use**:** Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into information systems. These devices are obtained from numerous sources and can contain malicious code that can be readily transferred to an information system through USB ports or other ports of entry. For these

reasons, sanitization of these devices is required prior to their initial use. Agencies shall develop procedures to support this requirement.

Logging and Accountability**:** Media must be logged throughout the media lifecycle, including creation, movement, and destruction, in accordance with applicable regulatory requirements. This media must be physically inventoried and accounted for at a predetermined interval as defined within applicable regulatory requirements.

IV. CORRECTIVE OR DISCIPLINARY ACTION

Each agency shall ensure that all relevant staff within their organizational authority are aware of and comply with this policy. The agency is responsible for enforcing it. Unauthorized and/or neglectful actions regarding this policy may result in disciplinary action up to and including dismissal. COT may require additional service charges for remediation efforts due to non-compliance with this policy.

V. APPLICABILITY

All executive branch agencies and non-executive branch agencies using COT-managed infrastructure or services shall adhere to this policy. This includes employees, contractors, consultants, temporaries, volunteers, and other workers within state government. Organizations may modify this policy to fulfill their responsibilities but must obtain approval through an exception request. Staff should refer to their internal policy that may have additional information or clarification.

VI. REFERENCES

Helpful references can be found on the Enterprise IT Policies webpage.