

**Office of the Chief Information Officer  
Enterprise Policy**

**Policy Number:** CIO-092

**Effective Date:** 10/07/2013  
**Reviewed Date:** 11/05/2014

**Subject:** Media Protection Policy

**Policy Statement:** 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 as defined in NIST Special Publication 800-53.

**Policy Maintenance:** The Office of the Chief Information Security Officer shall be responsible for the maintenance of this policy. Agencies may choose to add to this policy, in order to enforce more restrictive internal policies as appropriate and necessary. Therefore, staff members are to refer to their agency's related policy which may have additional information or clarification of this enterprise policy.

**Authority:** KRS 42.726 authorizes the Commonwealth Office of Technology (COT) to develop policies that support and promote the effective application of information technology within the executive branch of state government, as well as information technology directions, standards, and necessary management processes to assure full compliance with those policies.

**Applicability:** This policy is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, vendors and other workers within the Executive Branch of state government.

**Responsibility for Compliance:** Each agency shall be responsible for assuring appropriate staff members within their organizational authority are aware of the provisions of this policy, and that compliance by staff members is expected. It shall be each Executive Cabinet's responsibility to enforce this policy. Agencies may develop and enforce additional more restrictive procedures; however, the minimum standards identified by this policy are required.

**Review Cycle:** This policy will be reviewed at least every two years.

**Definitions:**

- Digital Media: Physical electronic media used to store information. (ex. diskettes, magnetic tapes, desktops, laptops, hard drives, random access memory, 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)

**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 [Enterprise Standard 5100: Encryption](#), 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 [Enterprise Standard 5100: Encryption](#), for enterprise standard requirements.

**Retention:** A media retention schedule shall be defined for all media in accordance with regulatory requirements. 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.

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

**Certification of Sanitization:** The sanitizing process shall be documented with the Commonwealth of Kentucky Record of IT Equipment Sanitization. A completed record must be maintained in a central location designated by the agency. 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 will 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 on a predetermined interval as defined within applicable regulatory requirements.

## References:

- NIST.SP.800-53r4.pdf , Security and Privacy Controls for Federal Information Systems and Organizations  
<http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>
- NIST Special Publication 800-88, Guidelines for Media Sanitization:  
[http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_with-errata.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf)
- National Security Agency, Media Destruction Guidance:  
[http://www.nsa.gov/ia/mitigation\\_guidance/media\\_destruction\\_guidance/index.shtml](http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml)

- Kentucky Department for Libraries and Archives, State Government Records Retention Schedules:  
<http://kdla.ky.gov/records/recretentionschedules/Pages/stateschedules.aspx>
- Enterprise Standards and Approved Products, 5100 Encryption:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-301110/>
- Enterprise Standards and Approved Products, 4080 Data Classification Standard:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-301107/>
- COT-F108, Commonwealth of Kentucky Record of IT Equipment Sanitization Form:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-381482/>

**\*END\***