THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY. THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.

SCDIS-501 Information Media Disposal Procedure

for all South Carolina state agencies

version: 1.0
issued: 01-Jul-2016
effective: 01-Jul-2016
owner:
Chief Information Security Officer
Division of Information Security
Department of Administration
State of South Carolina

A. Purpose

This Procedure establishes processes to be used by South Carolina state agencies to securely dispose of information media, of any format, as independent media or contained in any device.

This Procedure also establishes sanitization standards in Section E ("Overview of IT Hardware and Storage Media Sanitization Requirements") and Appendix C ("Procedures for Secure Erase Technology") that must be followed by all public bodies in South Carolina prior to the transfer or disposal of information technology hardware or storage media.

B. Scope

Per South Carolina Provisos 117.105 and 93.25 of the 2016-2017 Appropriations Act, and any successive provisos and statutes, this Procedure is to be implemented by all South Carolina state agencies, including institutions, departments, divisions, boards, commissions, and authorities. Exceptions are noted in the terms of the Provisos.

Within this scope, the Procedure set forth herein applies to:

1. all persons employed by or performing work for an agency, including but not limited to employees, contractors, and volunteers
2. all agency information systems, regardless of location or service level agreement
3. all information contained on any agency information system, regardless of format or medium
4. all information otherwise under the control of any agency, regardless of format or medium

C. Guiding Principles

These guiding principles should be used to assist in the interpretation of the objectives of all controls and processes described in this procedure and to assist in the implementation of this procedure by each agency.

1. **Confidentiality** – The primary objective of secure disposal of information media is to ensure that when information media are transferred sensitive information is not inadvertently transferred with it.
2. **Non-Obvious Locations** – Information media is located in many places that may not be obvious to all personnel. Devices such as printers and fax machines can easily be overlooked as containing information storage devices.
3. **Deletion is Not Secure Erasure** – In most cases, the contents of a file deleted through ordinary means will remain intact on the storage device.
4. **Information Security is Everyone's Responsibility** – All agency personnel are responsible for understanding these basic principles of information disposal, and when and how to follow this procedure.

D. Implementation

Each agency must determine the specific processes, tools, or services it will use to follow this Procedure and must ensure that any service provider it uses complies with this Procedure.

E. Overview of IT Hardware and Media Sanitization Requirements

External Transfer and Disposal

Pursuant to South Carolina Code Ann. § 30-2-310(B), before a "public body"[1] may transfer or dispose of information technology hardware or storage media owned or leased by it, the hardware and storage media must be sanitized in accordance with standards and policies adopted by the Department of Administration. The sanitization standards that have been adopted by the Department of Administration are set forth in the attached *Appendix C- Procedures for Secure Erase Technology*. All public bodies must sanitize hardware and storage media in accordance with these sanitization standards and procedures prior to transfer or disposal of such equipment.

Staff personnel should always consult with their IT department prior to disposing of any computer equipment. IT departments can assist in the proper sanitization of equipment before disposal or transfer.

The director or appropriate information technology manager of a public body must complete and sign a certification that the hardware has been properly sanitized before it can be surplused, transferred, donated or junked. Copies of all certification statements must be maintained by the agency's IT staff and provided to the State's Surplus Property Office when appropriate. A sample sanitization certification form can be found at the State's Surplus Property Office website at http://www.admin.sc.gov/generalservices/surplus/State-Program/State-Agency-Documents.

[1] "Public body" is defined by South Carolina Code § 30-1-10(B) to mean "any department of the State, any state board, commission, agency, and authority, any public or governmental body or political subdivision of the State, including counties, municipalities, townships, school districts, and special purpose districts, or any organization, corporation, or agency supported in whole or in part by public funds or expending public funds, including committees, subcommittees, advisory committees, and the like of any such body by whatever name known, and includes any quasi-governmental body of the State and its political subdivisions, including, without limitation, bodies such as the South Carolina Public Service Authority and the South Carolina Ports Authority."

Internal Transfer or Reassignment

Any computing hardware is likely to contain sensitive information left from the previous user such as passwords and human resources information within operating system files, cached email, or browser cached web pages that should not be accessible to others. Therefore, information technology hardware or storage media that is to be transferred internally within an organization through reassignment to a new user, or that is to be inventoried due to a break in service, must be properly sanitized in accordance with the standards set forth in *Appendix C- Procedures for Secure Erase Technology.*

F. Procedure for Facilities Staff

1. To provide for the secure destruction of any media that cannot be securely erased, **procure ongoing services and/or facilities** to destroy such media commonly used by the agency.
2. To ensure all persons within the stated scope of this Procedure understand the relevant secure processes they are to follow:
   a. Initially place, and periodically confirm that **signage at all destruction service drop locations** remains visible and legible. *See Appendix A.*
   b. Annually send **communication to all persons within scope (*see section B. Scope*)**, providing guidance on secure media destruction processes. *See Appendix B*.
3. To confirm that persons are properly following processes, periodically **visually check other disposal collection points** (e.g., central trash and recycling collection) for the presence of sensitive information media.

G. Procedure for Agency Desktop and Server Administration Staff

1. To prepare for secure disposal of information storage media, **document the processes to follow and tools to use** to securely erase computing devices and information storage devices (*See Appendix C- Procedures for Secure Erase Technology*). These processes and tools must account for all computing devices and information storage devices commonly in use, such as:
   - computers
   - magnetic hard drives
   - solid state hard drives
   - flash memory cards and drives
   - printers
   - optical storage devices
   - cellular phones
   - handheld computing devices
2. When a **computing device or information storage device is repurposed or reassigned**, that device must first be securely erased.

H. Procedure for Agency Supervisors

1. To ensure all agency personnel understand the relevant secure processes they are to follow, during onboarding, agency supervisors must **confirm that all new agency employees have read and understand the guidance on secure media destruction processes**. See *Appendix B*.

I. Procedure for All Agency Personnel

Prior to disposal of information, state agencies and their employees are responsible for ensuring that erasure or destruction of the information contained therein complies with any applicable state and agency records retention schedules. If guidance or assistance is needed in this regard, agencies may contact the South Carolina Department of Archives and History. (http://rm.sc.gov)

1. **Non-Public by Default:** Start by assuming that any information medium (hard copy or electronic) contains non-public information. Unless you are certain all of the information is public (see I.2.), treat it as non-public. Any non-public information medium must be disposed according to the following process:

a. **If it's paper, shred it:** If it is paper or paperboard medium, personally deliver it to the locked shred bin or put it through a cross cut shredder approved by agency facilities staff.
b. **If it's CD or DVD, shred it:** If it is a CD or DVD medium, personally deliver it to the locked shred bin or put through a shredder approved for CD/DVD shredding by agency facilities staff.
c. **If Rewriteable, Securely Erase It:** If it is a rewriteable medium (e.g., hard drive, flash drive), ensure it is securely erased by agency personnel who are trained to perform secure erasure. Once the medium is securely erased, it can be disposed in the same way a public information medium is disposed (see I.2).

2. **Public Information Medium:** An information medium can only be considered as public if all information present on it is intended or required to be shared with the public. **Use Caution:** In normal use of electronic media, especially rewriteable electronic media, previously written information may not be fully overwritten by current information. Therefore, rewriteable media should in most cases be treated as containing non-public data. **Examples of public information include:** publicly distributed information, agency pamphlets and brochures, press releases, agency contact information, and public website information.

   a. For IT hardware assets, follow agency and State Surplus Property Office policy for proper disposal of such items. By law, State owned property must be disposed of through the State's Surplus Property Office. Computer related hardware must be sanitized in accordance with *Appendix C- Procedures for Secure Erase Technology* and be documented in the *Surplus Property Turn-In Document*. Guidance and forms are available on the State Surplus Property Office website: http://www.admin.sc.gov/generalservices/surplus/State-Program/State-Agency-Documents

   b. For Other Public Information Media, Recycle or Discard: If an information medium is known to be blank, or to contain only public information, that medium may be recycled or discarded, as appropriate.

J. Additional Guidance

For additional guidance on media sanitization, consult NIST Special Publication 800-88, *Guidelines for Media Sanitization*.

K. History

Date	Version	Author: Description
01-Jul-2016	1.0	Division of Information Security: Created with guidance from NIST Special Publication 800-88 "Guidelines for Media Sanitization"

Drop-Off for Shredding

Place materials in the slot in the top of the gray bin.

Materials deposited here MAY NOT BE RETRIEVED.

Shredding schedule: weekly on Mondays

Paper

- Staples OK
- Remove paperclips
- Remove spiral metal bindings

Paperboard

- Same as paper

CDs & DVDs

- Deposit discs only, no cases.

Per state policy, all paper, CD, and DVD media containing non-public data must be shredded before disposal. Deposit these items in the slot at the top of the gray bin for shredding.

Appendix B – Example Annual Email Reminder

Subject: Secure Disposal of Information Media

To all agency personnel:

When disposing of Paper, CDs, DVDs

In general, these media must be disposed by shredding. Deposit these in person, in one of the gray shred bins (see shred bin locations below). Staples may be left in printed documents; but remove paperclips, spiral metal bindings, and similar sturdy metal parts.

These media do not have to be shredded if you know with certainty that they only contain information that is publicly available elsewhere. Examples: publicly distributed information, agency pamphlets and brochures, press releases, and, printed public website information.

Shred bin locations

A. [description of location 1]
B. [description of location 2]

Shredding Schedule

Shredding is done weekly on Mondays. When Monday is a holiday, shredding is done on the next business day following.

Shredding is performed on site by contractor *[vendor name]*, and is monitored by agency staff members.

When disposing of Diskettes, Flash Drives, Hard Drives, Cell Phones, Printers, Computers

Contact [help desk] ([help desk contact info]) for assistance.

Appendix C – Procedures for Secure Erase Technology

Hard Drive Erasure

At a minimum, to securely erase a hard drive, overwrite the entire writeable surface area with a single pass of binary-zero data. This may be done by software or by hardware.

Most hard drives use an automatic "sparing" process that transparently substitutes hidden outer tracks for malfunctioning inner tracks. For more stringent security requirements, special hardware drive erasure tools are available to overwrite these spared tracks.

A hard drive that has become unwriteable may be erased with a degaussing (demagnetizing) tool specifically designed for hard drive erasure. Alternatively, the hard drive may be physically destroyed using a hard drive crusher.

Note that depending on the data stored on the drive (e.g., IRS, CJIS, DoD), more advanced erasure processes may be required for compliance with federal or contractual obligations. Consult the relevant compliance guidelines.

Diskette Erasure

Diskettes should be erased using a degaussing (demagnetizing) tool.

Because of imprecise diskette drive tracking, overwriting should not be considered a secure method of erasing diskettes.

Note that depending on the data stored on the diskette (e.g., IRS, CJIS, DoD), more advanced erasure processes may be required for compliance with federal or contractual obligations. Consult the relevant compliance guidelines.

Flash Drive / Solid State Drive Erasure

Flash memory drives (USB thumb drives, Solid State Drives, etc.) should be erased using software or hardware specifically designed to invoke the built-in ATA Secure Erase mechanism, or similar hardware-level erase function.

Caution: Flash memory technology has limitations on the number of times it can be written and rewritten. To work around this limitation, flash memory drive makers typically employ an algorithm for remapping drive sectors to varying memory locations during drive usage. Because of this remapping, standard overwriting erasure software will not reliably overwrite all data storage locations.

Caution: Flash memory generally does not respond to degaussing (demagnetizing). This technique should never be used on flash memory drives.

Note that depending on the data stored on the drive (e.g., IRS, CJIS, DoD), more advanced erasure processes may be required for compliance with federal or contractual obligations. Consult the relevant compliance guidelines.

Smartphone and Handheld Device Erasure

The process required to perform secure erasure of a smartphone or other handheld device will vary by operating system. Some examples are described below:

Apple iOS: The built-in device "Reset" process, when using the option to erase all device content and settings, will satisfy state requirements in most circumstances.

Android: In current versions of Android OS (as of this writing), the built-in device reset process does not reliably overwrite storage. To ensure that data is not recoverable, the device must first be fully encrypted using a complex passphrase, and then reset using the built-in reset operation. Note that any removable SD storage medium must be securely erased by removing it and performing a secure erasure externally (see Flash Drive / Solid State Drive Erasure process above).

Note that depending on the data stored on the device (e.g., IRS, CJIS, DoD), more advanced erasure processes may be required for compliance with federal or contractual obligations. Consult the relevant compliance guidelines.