COMPLIANCE COMPONENT

DEFINITION	
Name	Disposal Phase
Description	The disposal phase ensures the appropriate sanitization of agency information. Sanitization is the process used to remove data from information systems and media such that there is reasonable assurance that it cannot be retrieved or reconstructed.
Rationale	The disposal phase is essential to prevent the inadvertent release of information and/or software.
Benefits	• Protects sensitive information from disclosure. • Adheres to copyright, statutory, and regulatory requirements.

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	System Life Cycle Security
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	

State the Guideline, Standard or Legislation	• Hard Copy Media are physical representations of information, most often associated with paper printouts.
	• Hard Copy Media can be disposed of by either incineration or shredding (provided the shredded material is of appropriate size according to agency requirements).
	• Electronic media includes, but is not limited to, the following:
	  ○ Magnetic tape or disk
	  ○ Optical media
	  ○ Hard disk drives
	  ○ Solid state drives
	  ○ USB drives
	  ○ Copiers
	  ○ Fax machines
	  ○ Printers
	  ○ Scanners
	  ○ Mobile devices (cellphones, tablets, etc.)
	  ○ Memory cards
	• Official electronic records shall be properly archived or disposed using agency approved methods.

	• Obsolete, surplus or decommissioned media containing agency data shall be overwritten, degaussed or destroyed.
	• A record shall be kept of who, when, and how sanitization or disposal actions were implemented on all electronic media and the final disposition of such media shall be maintained within the agency for an appropriate length of time.
	• If the sanitization status of electronic media is unknown, it shall be considered not to have been overwritten, degaussed or destroyed.
	• The information owner shall be responsible for backing up any data to be retained before allowing the media to be disposed.
	
	<u>Overwriting Electronic Media</u>
	
	• Overwriting electronic media should only be used if destroying or degaussing is deemed impractical by appropriate authorities.
	• If damaged electronic media inhibits the overwriting process, the media shall be physically destroyed or degaussed.
	• Overwriting software shall provide the capability to:
	  ○ Purge all data or information, including the O/S, from the physical or logical drives.
	  ○ Overwrite all sectors, blocks, tracks, and slack or unused space on the entire medium.
	  ○ Individually wipe Raid controlled hard drives.
	  ○ Verify that all data has been removed from the entire electronic media.
	  ○ Provide the user with validation that the procedure was completed properly.
	• Overwriting software that merely reformats or repartitions a hard drive is not acceptable.
	• The overwriting process shall be performed at least three times before verifying the media is sanitized.
	
	<u>Destroying Damaged Electronic Media</u>
	• Damaged media under maintenance agreements may be returned to the vendor if appropriate non-disclosure agreements have been signed and all agency data has been wiped.
	• Electronic media may be physically destroyed by one of the following methods:
	  ○ Disintegrate, pulverize, melt, incinerate or shred the media so that it cannot be re-used as a functioning device.
	
	<u>Degaussing Electronic Media</u>
	• The degausser shall be rated sufficient for the media.
	• Shielding materials may be removed from the hard drive and magnetic platters may be removed from the hard drive housing before degaussing.
	• Individuals performing the degaussing function shall be properly trained.

Document Source Reference #	NIST SP 800-88 Guidelines for Media Sanitization, Rev. 1 (www.csrc.nist.gov/publications/nistpubs); DOD 5220.22-M, National Industrial Security Program Operating Manual

Compliance Sources			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

KEYWORDS	
List Keywords	Wipe, erase, clean, expunge, obliterate, purge, surplus, confidential, sanitize, shred, degauss

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

COMPONENT SUB-CLASSIFICATION		
Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	

Migration Strategy	
Document the Migration Strategy	

Impact Position Statement	
Document the Position Statement on Impact	

CURRENT STATUS				
Provide the Current Status	☐ *In Development*	☒ *Under Review*	☒ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	07/22/2004	*Date Approved / Rejected*	04/18/2019
Reason for Rejection			
Last Date Reviewed	02/01/2022	*Last Date Updated*	02/23/2022
Reason for Update	Vitality		