NDMA

NATIONAL DATA
MANAGEMENT AUTHORITY

Sanitisation/Secure Disposal Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This standard establishes controls for the secure disposal of storage media and devices.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorised disclosure of information and to ensure its confidentiality.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It specifically addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

As per the Information Security Policy, information must be properly managed from its creation, through authorised use, to proper disposal.

The organisation must ensure that users and custodians of information are aware of its sensitivity and the basic requirements for media sanitisation and secure disposal.

The organisation must ensure that all workforce members, including property management and custodial staff, are made aware of the media sanitization and secure disposal process in order to establish proper accountability for all data.

The organisation must ensure that confidential material is destroyed only by authorised and trained personnel, whether in-house or contracted, using methods outlined in this standard.

The organisation may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard. The organisation must ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the information classification standards.

4.1 Methods of Media Sanitisation

The following table depicts the three types of sanitisation methods and the impact of each method.

Sanitisation Method	Appropriate Use	Description
Clear	If the media will be reused and will not be leaving the organisation's control.	Protects confidentiality of information against an attack by replacing written data with random data. Clearing must not allow information to be retrieved by data, disk or file recovery utilities.
Purge	If the media will be reused and leaving the organisation's control.	Protects confidentiality of information against an attack through either degaussing or Secure Erase.
Physical Destruction	If the media will not be reused at all.	Intent is to completely destroy the media.

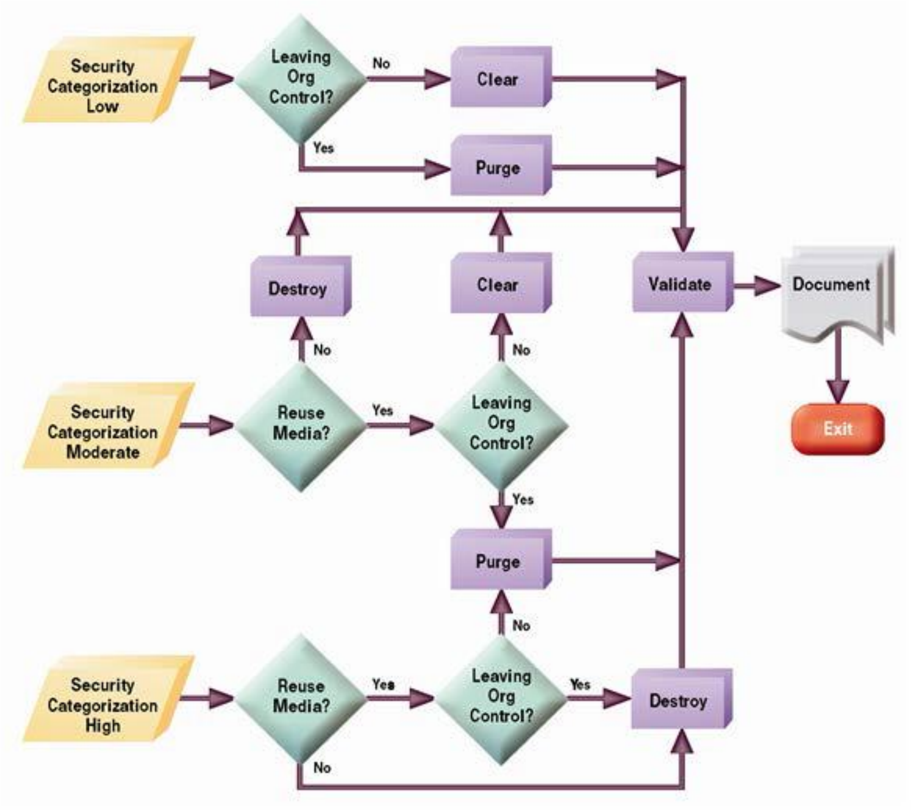
4.2 Sanitisation Decision Process

The decision process is based on the confidentiality of the information, not the type of media. The organisations choose the type of sanitisation to be used, and the type of sanitisation is approved by the Information Owner. The technique used may vary by media type and by the technology available to the custodian, so long as the requirements of the sanitisation type are met. Recommended Sanitisation techniques for specific types of media are outlined in Appendix A of NIST 800-88, Rev. 1, Guidelines for Media Sanitisation, Minimum Sanitisation Recommendations. [1]

Disposal without sanitisation should be considered only if information disclosure would have no impact on organisational mission, would not result in damage to organisational assets, and would not result in financial loss or harm to any individuals.

The security categorisation of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on media type.

[1] NIST Special Publication 800-88 Revision 1
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf



Sanitisation and Disposition Decision Flow (*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)

The cost versus benefit of a sanitisation process should be understood prior to a final decision. Organisation can always increase the level of sanitisation applied if that is reasonable and indicated by an assessment of the existing risk. For example, even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options. Entities may not decrease the level of sanitisation required.

4.3 Control of Media

A factor influencing a sanitisation decision is who has control and access to the media. This aspect must be considered when media leaves organisational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organisation. The following are examples of media control:

Under Organisational Control:

4.3.1 Media being turned over for maintenance are still considered under the organisation’s control if contractual agreements are in place and the maintenance provider specifically provides for the confidentiality of the information.

4.3.2 Maintenance being performed on an organisation's site, under the organisation's supervision, by a maintenance provider is also considered under the control of the organisation.

Not Under Organisation Control:

4.3.3 Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organisation are considered to be out of the organisation's control.

4.4 Reuse of Media

Organisation should consider the cost versus benefit of reuse. It may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options.

Clear / Purge / Destroy

Method	Description
Clear	One method to sanitise media is to use software or hardware products to overwrite user- addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user- addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating,

Method	Description
	degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

Sanitization Methods (*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)

4.5 Validation

Organisation must test a representative sampling of media for proper sanitisation to assure that proper protection is maintained.

4.6 Verification of Equipment

If the organisation is using sanitisation tools (e.g., a degausser), the organisation must have procedures to ensure that the tools are operating effectively.

4.7 Verification of Personnel Competencies

Organisations must ensure that equipment operators are properly trained and competent to perform sanitisation functions.

4.8 Document

Organisation must maintain a record of their sanitization to document what media were sanitised, when, how they were sanitised, and the final disposition of the media.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the standard may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
Sanitisation[1]	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Authorised[2]	A system entity or actor that has been granted the right, permission, or capability to access a system resource.
Unauthorised Access[3]	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Security Categorisation[4]	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Cryptographic Erase[5]	A method of sanitization in which the media encryption key (MEK) for the encrypted Target Data is sanitized, making recovery of the decrypted Target Data infeasible.
User[6]	Individual or (system) process authorized to access an information system.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[2] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/authorized

[3] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/unauthorized_access

[4] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/security_categorization

[5] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/cryptographic_erase

[6] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user