Eskom	Guideline	Distribution, Transmission & Generation

Title: **SANITISATION AND DISPOSAL OF STORAGE MEDIA**

Unique Identifier:	**240-110767932**
Alternative Reference Number:	**n/a**
Area of Applicability:	**Engineering**
Documentation Type:	**Guideline**
Revision:	**Draft 1.1**
Total Pages:	**21**
Next Review Date:	**June 2028**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Meenal Vala	**Nosipho Bodlingwe**	**Mervin Mottian**
OT Cybersecurity Care Group Chair	**Smart Grid SC Chair**	**Tx IM Snr Manager Information & Cybersecurity**
Date:	Date:	Date:

Authorized by	Authorized by	Supported by SCOT/SC
Ezzard De Lange	**Christoph Kohlmeyer**	**Nelson Luthuli**
Dx Snr Manager IT, OT Cybersecurity	**Gx Snr Manager C&I**	**SCOT/SC Chairperson**
Date:	Date:	Date:

SCOT Study Committee Number/Name: **Smart Grid Study Committee**

Content

Figures

Tables

1. Introduction

Sanitisation of cyber assets in Eskom is important to ensure that sensitive information does not leave the business unintentionally. If sanitisation is neglected, it places the business at risk by having classified information falling in the hands of 3rd parties and possible malicious actors. This is often a neglected area as it is either not done or not implemented correctly. This document will aid system owners in identifying the correct level of sanitisation and the correct procedure for that sanitisation method. System owners shall use this guideline to choose the correct sanitisation method to dispose of information stored on storage media prior to maintenance, redeployment, decommissioning or disposing of a cyber-asset.

2. Supporting clauses

2.1 Scope

This document will cover the following media:

- Hard Copy Storage
- Routers and Switches (including modems)
- Mobile Devices
- Floppies
- Cassettes
- Compact Disks and DVDs
- AT hard drives
- SCSI hard drives
- ATA solid state drives
- SCSI solid state drives
- Externally located flash hard drives
- USB removable media
- Memory cards
- Office Equipment
- Substation Equipment
- RAM and ROM-based Storage Media
- Optical Media Sanitisation

2.1.1 Purpose

Storage media sanitisation prior to the disposal or re use of cyber assets is critical to ensuring the protection of Eskom information. This is to prevent unauthorised access to Eskom information after the disposal of an Eskom cyber asset.

This guideline supports the following requirement as per the Cyber Security Standard for operational Technology [1] “Equipment that are decommissioned shall be sanitised before disposal. A procedure that describes the process shall be available and followed.”

This document recommends the method of sanitising different storage media types in Operational Technology as well a use of approved disposal methods of the sanitised media.

2.1.2 Applicability

This document shall apply to the Operational Technology environments throughout Eskom Holdings Limited Divisions.

2.2 Normative/informative references

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] 240-55410927 – Cyber Security Standard for Operational Technology

[2] 32-438 – Information Security Systems Classification

[3] National Institute of Standards and Technology (2014, December). 800-88 Guidelines for Media Sanitization Rev 1 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

2.2.2 Informative

[4] 32-245 Eskom Waste Management Standard

[5] The National Intelligence Agency (1996). Minimum Information Security Standard [Online].Available: http://www.kzneducation.gov.za/DocumentsPublications/Policies/General.aspx

2.3 Definitions

2.3.1 General

Definition	Description
Clear	A method of sanitisation by applying logical techniques to sanitise data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). [3]
Destroy	A method of sanitisation that renders target data recovery infeasible using state of the art laboratory techniques and results in subsequent inability to use the media for storage of data.[3]
Dispose	To get rid of something that cannot be reused. This will refer to media that has been sanitised by destruction and components need to be discarded appropriately as e-waste.
DoD Short	Department of Defence (DoD) Short is the term given of writing a pseudorandom pattern to a device with 3 passes. This is one of the purge methods recommended by the NIST sanitisation guideline [3].
E-waste	Electric or electronic devices or components that have reached the end of their life cycle and have thus been sanitised and need to be disposed of.

Definition	Description
Hard disk	Hard Disk Drive (HDD), often called “hard drive” or “hard disk”, is a data storage device used for storing and retrieving digital information using one or more rigid rapidly rotating disks coated with magnetic material. HDDs are a type of non-volatile memory that retains stored data even when powered off.
IDE/ATA Hard Disk	Parallel ATA use an IDE/ATAT connector between hard disks and computers. Designed in 1986 and were superseded by Serial ATA (SATA) in 2003. The bandwidth varied between 33 – 133 MB/s
Microforms	Microforms are any forms, either films or paper, containing micro reproduction of documents for transmission, storage, reading, and printing.
NIST 800-88 “Guidelines for Media Sanitization”	The international guideline from the National Institute of Standards (NIST) and Technology for securely sanitising storage media.
Peripheral devices	A device that is used up transfer information in or out of a computer.
Purge	A method of sanitisation by applying physical or logical techniques that should render target data recovery infeasible using state of the art laboratory techniques. [3]
Recycle	Means a process where waste is reclaimed for further use, which process involves the separation of waste from a waste stream for further use and the processing of that separated material as a product or raw material.
SCSI	Small Computer System Interface (SCSI) is a set of standards connecting and transferring data between computers and peripheral devices.
Serial ATA	Serial ATA (SATA) superseded Parallel ATA from 2003. The bandwidth various between 150 – 1969 MB/s
Solid State Drive	A non-volatile storage device that stores persistent data on solid-state memory.
Standard DoD 5220.22-M	The standard for the department of defence that writes a pseudorandom pattern for 7 passes to a hard drive. The DoD Standard was never an official standard and has been superseded by the NIST sanitisation guideline [3].
Storage Media	Storage media are devices that store application and user information. Examples are HDD/SDD/ATA, etc.
System Owner	The system owner is the authorised Eskom representative that has overall accountability for the Operational Technology system in which the cyber asset resides.[1]

2.3.2 Disclosure classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description
ATA	Advanced Technology Attachment
BB	Blackberry
BD	Blue-ray Disc

Abbreviation	Description
CD	Compact Disc
DoD	Department of Defence
DRAM	Dynamic Random Access Memory
DVD	Digital Versatile Disc
EAPROM	Electronically Alterable Programmable Read-Only Memory
EEPROM	Electronically Alterable Programmable Read-Only Memory
HDD	Hard Disk Drive
IDE	Integrated Drives Electronics
MB/s	Mega Bytes per second
MEK	Media Encryption Key
NIST	National Institute of Standards and Technology
NVM	Non-Volatile Memory
OS	Operating System
OT	Operational Technology
RAM	Random Access Memory
ROM	Read Only Memory
SATA	Serial ATA
SCSI	Small Computer System Interface
SSD	Solid State Drive

2.5 Roles and responsibilities

The implementation of this guideline is the accountability of the Eskom OT system owners. The Eskom OT system owners may delegate the responsibility of the implementation of this guideline

2.6 Process for monitoring

Implementation shall be done by the relevant systems Owner in OT. The OT Cyber Security Care Group is responsible for updating this guideline.

2.7 Related/supporting documents

Not applicable.

3. Storage Media Sanitization Process Flow

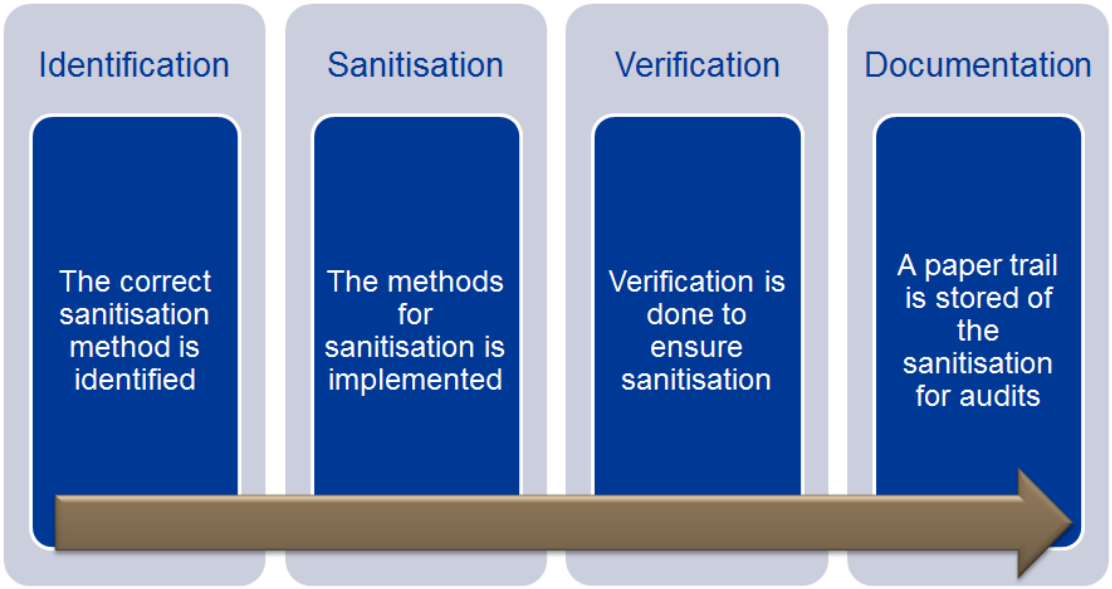

Figure 1: Process flow

This document will help system owners identify which sanitisation method to use. Then the system owner will sanitise the storage media. Verification is then done to ensure the storage media was sanitised correctly. Finally, documentation of the sanitisation process is recorded for audits by completing and storing the Certification of sanitisation (Appendix A).

3.1 Classification of Data

Data that resides on storage media require a security classification/categorisation. This is in compliance to the Cyber Security Standard for Operational Technology [1]. The system owner is responsible for ensuring data is classified. The NIST 800- 53 recommends the utilisation of 3 categories for the potential adverse impact level of unauthorised disclosure of Data, namely, Low impact (limited adverse effects), moderate impact (serious adverse effects) and high impact (severe or catastrophic adverse effects)

Data shall be classified according to their sensitivity and description as follows:

a) **Unclassified/Public Domain (low):** can be released to the public and general availability within the business. No impact from data disclosure.

b) **Controlled/Internal disclosure (moderate**): information is company-wide and should be protected with limited controls. Controlled disclosure documents and data may include various standards, policies and Eskom wide memos. It can also be classified as general business communication, non-operational data that can be shared within the business without higher levels of clearance and can be made available to External parties when requested and approval is given to allow access to the Data. Low impact to the disclosure of data.

c) **Confidential Data (moderate/high**): (OT communications, non-operational data that could affect operations if disclosed, field data for historian and analytics for Tx and Dx) Classification allocated to all information that may be used by malicious, opposing, hostile elements to harm the objectives and function of an individual and/or an institution. Compromise thereof can lead to the disruption of cyber assets essential to the reliable operation of critical plant assets which are those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network affecting a specific area, region or customer base and/or compromise the stability and availability of the grid. This would also relate to the damage/loss to critical plant assets >400MW if the breach would cause the deliberate destruction or failure of said plant. This would extend to any deliberate or unintended danger to persons. Moderate impact to disclosure of data.

d) **Secret Data (high**): (All power network OT data: SCADA/CNI and Automation data that allows control) Classification allocated to all information that may be used by malicious, opposing, hostile elements to disrupt the objectives and function of an institution and/or state.

Compromise thereof can lead to the disruption of Cyber assets essential to the reliable operation of critical plant assets which are those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network affecting a large area, region or distribution customer base and/or compromise the stability and availability of the grid for an extended period. This would also relate to the damage/loss to critical plant assets of >800MW if the breach would cause the deliberate destruction or failure of said plant.

Compromise thereof can also disrupt the effective execution of operational plans; can damage operational relations between the Transmission and Distribution operators; can endanger the public. Moderate to high impact to disclosure of data.

e) **Top Secret Data (High):** (SCADA, Automation and Plant data at Gx) Classification allocated to all information that may be used by malicious, opposing, hostile elements to neutralise the objectives and function of an individual and or an institution. Compromise thereof can disrupt the effective execution of operational plans; Can seriously damage operational plans between institutions; Can lead to the discontinuation of diplomatic relations between states; can result in declaration of war.

Compromise thereof can lead to the disruption of Cyber assets essential to the reliable operation of critical plant assets which are those facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electricity supply network affecting the country and/or compromise the stability and availability of the grid for an extended period resulting in complete black out. This would also relate to the damage/loss to critical plant assets >4000MW if the breach would cause the deliberate irreparable destruction or failure of said plant and would require extensive time for repair and return of operations.

Compromise thereof can disrupt the effective execution or operational plans of the business; can disrupt the effective functioning of the grid; can damage the governing of the country; can endanger the public. High impact to the disclosure of data.

3.2 Default Classification

Where a system classification has not been assigned, a default classification of Confidential shall be assumed for the system and its subsystem components. [2] Therefore, all data residing on storage media shall be considered confidential until a classification is given.

3.3 Data Classification Period

Once a disk obtains a certain level of categorisation of data, it cannot be lowered until the storage media is sanitised.

Example, if a “secret” document is copied then deleted on a storage media, the level of categorisation for the storage media will remain at “secret” until it has been sanitised and certificate is kept on record. This is because in most cases of storage methods, storage media removal and deletion do not delete data, but remove pointers to the data and the data will still reside on the storage media. Since it is unsure when the data will be sufficiently overwritten in normal operations, it will be treated at its highest level of categorisation during its operational history until sanitisation.

Figure 2 below shows a summary for security classification and the decision flow.

3.4 Methods of Sanitisation

Sanitization of data storage media involves the process of securely erasing or destroying data on storage devices to prevent unauthorized access to sensitive information. The NIST Special Publication 808-88: Guideline for Media Sanitisation [3] defines three sanitisation methods:

1) **Clear:** Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. Clearing applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state.

   a) The NIST Clear method uses standard read/write commands, techniques and tools to overwrite all the user-addressable locations including logical file storage locations on an ATA hard drive or SSD with non-sensitive data (binary 1s and 0s). The Clear pattern for media overwriting should include at least a single write pass with a fixed data value such as all zeros. Multiple write passes or values that are more complex may optionally be used.

Note: Overwriting on SSDs (flash storage) may reduce the effective lifetime of the media. Also, it may not sanitize the data in unmapped physical media.

2) **Purge:** Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack through the use of physical or logical techniques. For some media, clearing media would not suffice for purging. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and specially trained personnel.

   Examples of purge techniques:

   a) **Overwrite** - The Purge method uses the overwrite EXT command to overwrite – i.e. apply a single write pass of a fixed pattern (all 0s or a pseudorandom pattern) – on ATA hard disk drives. Optionally, it may apply three total write passes of a pseudorandom pattern (DoD Short) so that the second write pass is the inverted version of the original pattern. This involves overwriting the data on the storage device with random data to make it difficult or impossible to recover the original data. This method can be performed using software tools **or specialized equipment.**

   b) **Block erase** - is the secondary erasure method for SSDs, which "electrically" erases each block by using internal SSD functions. After successful implementation of the block erase command, the method applies binary 1s across all the user-addressable locations on the storage media and then repeats Block Erase.

   c) **Crypto / secure erase** - use of Cryptographic Erase command to sanitize ATA hard drives and SSDs that support encryption. This involves encrypting the data on the storage device with a strong encryption algorithm, rendering the data inaccessible without the encryption key. To securely sanitize the device, the encryption key must be securely deleted or destroyed.

d) **Degaussing (non-destructive) -** Degaussing qualifies to be a purge technique under NIST guidelines only if the sanitized media is available for reuse after it is purged. If the device is no longer available for use, such degaussing is considered as a destroy technique.

3) **Destroy (Hardware Destruction and Disposal):** Destruction of media is the **ultimate form of sanitization**. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting to render data irretrievable. Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data. While useful in cases where drives are irreparable or unable to be erased, physical destruction can be harmful to the environment and financially costly. This is because physical destruction of data storage hardware destroys the assets so they are unable to be reused or resold, shortcutting the lifespan of functional devices. Methods of media destruction:

a) **Disintegration** – the physical destruction method of disassembly of the device into components and destruction of said components to allow reassembly impossible. Components can be destroyed with methods listed below.

b) **Incineration** – Destruction of media through burning the media completely to ash.

c) **Pulverizing** - Destruction of media by force to make reconstruction and usage impossible. Lower cost option is to disassemble the device and only pulverise the key components. Methods of pulverization are but not limited to:

d) **Shredding** - Destruction of media through cutting or tearing into smaller pieces.

e) **Melting** - Destruction of media through changing form from solid to liquid state through the application of heat.

f) **Degauss (destructive):** is a form of physical destruction whereby data is exposed to the powerful magnetic field of a degausser and neutralized, rendering the data unrecoverable. Degaussing can only be achieved on hard disk drives (HDDs) and most tapes, but the drives or tapes cannot be re-used upon completion. Degaussing is not an effective method of data sanitization on solid state drives (SSDs).

3.5 Internal Destruction Methods

Special consideration must be given to the situation the business is currently facing in terms of financial constraints and the ability to obtain contracts and vendors to adequately sanitise media. A low-cost sanitisation option to destroy media can be used.

Many business units have access to engineering/mechanical workshop facilities that would allow for these low-cost media destruction options to be performed safely within the business. It is important to follow proper safety procedures when using these methods to avoid injury and ensure witnessing of destruction is observed and records are completed and filed. The task should also be performed by a trained technician to utilise said tool and work should be conducted under a task order. Guidance should be given to assist the technician in perform the function correctly, ensuring the storage media is adequately destroyed.

Examples to each of the destruction method are listed below:

a) **Incineration** – This method is preferably done through a vendor or authorised service provider with the correct methods to incinerate the storage media. It is not recommended for safety and environmental factors that incineration be performed without the correct method and tools (i.e., do not dispose of the media by burning it in a barrel).

b) **Melting** - This method is preferably done through a vendor or authorised service provider with the correct methods to melt the storage media. It is not recommended for safety and environmental factors that melting be performed without the correct method and tools.

Below are the preferred methods of media destruction that are applicable internally (non-contract):

a) **Disintegration** – Disassemble the storage media to as many pieces as possible. The non-storage components can be disposed of as general e-waste or recycled. The core storage media components need to be destroyed to prevent re-assembly. Destruction methods listed below can be used for these core components.

b) **Shredding** - This method is preferably done through a vendor or authorised service provider with the correct shredders. It is not recommended that normal office shredders be used expect for their intended use which is the shredding of paper.

1) Shredding through grinding or cutting is low budget method involving the use of workshop power tools to cut the media into small pieces. This can be done for most media before or after disintegration.

c) **Pulverizing** – This method is best performed after the media storage has been disintegrated and only the core media storage components are pulverised. This can be performed safely under a task order by an Eskom mechanical workshop by either grinding the components, hammering or drilling through the components with a drill press or shattering.

1) Hammering: A low-budget option for media destruction is to use a hammer or mallet to smash the media into small pieces. This can be done for hard drives, CDs, and DVDs, and is effective in rendering the media unreadable.

2) Drilling: Using a power drill to make several holes through a hard drive or CD/DVD can also render the data unreadable. This method can be effective and low-cost, but it is important to ensure that the drill goes through all parts of the media to prevent any data from being recoverable.

d) **Degauss (destructive):** Degaussing is the cleanest, most cost-effective, and efficient method of data sanitization. After degaussing, the data is not recoverable and no longer exists, leaving the media safe for recycling or disposal.

3.5.1 Identification of Method of Sanitisation

The figure below shows the recommended flow to determine the sanitization method for the cyber asset.

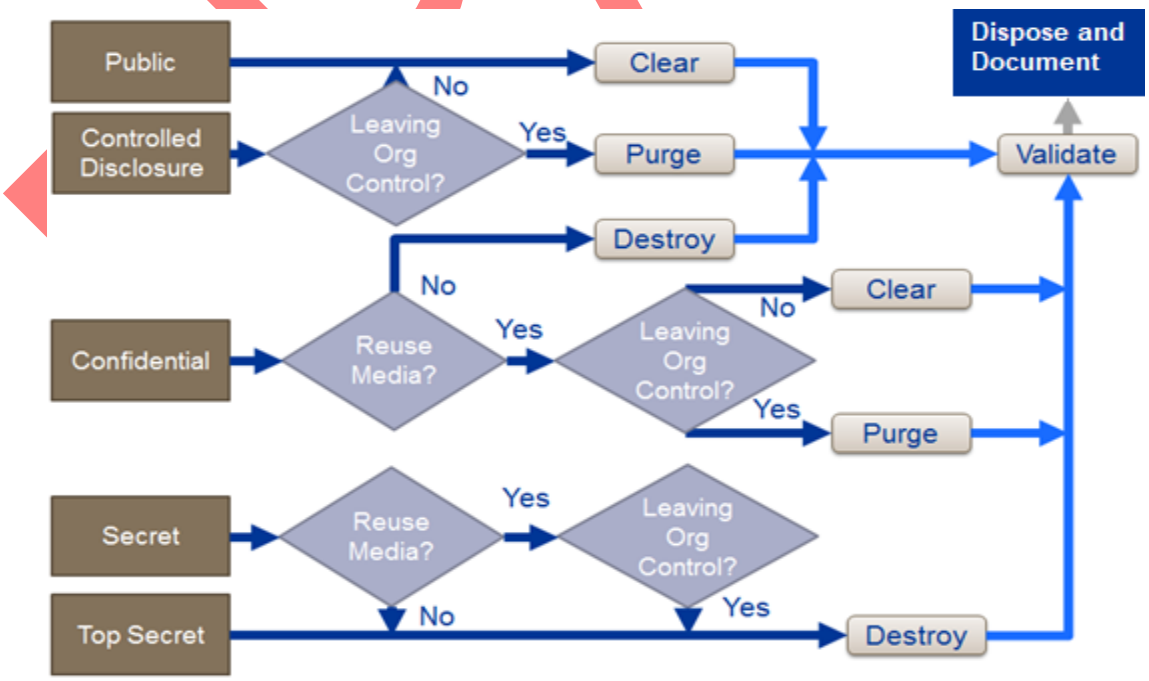

Figure 2: Sanitisation decision flow graph

a) In the case where a method is not available, then the next level of sensitisation will be used (example, if no purge method is available, the method will be upgraded to destroy)

b) While most devices support some form of clear, not all devices have a reliable purge mechanism.

c) Purge may be more appropriate than destroy when factoring in environmental concerns and business efficiency through recycling cyber assets as well as cost saving measures to reuse said media.

Prior to sanitisation, the system owner shall decide if the storage media will be reused in Eskom or will leave the organisation. Clean and purge methods shall be used to allow storage media to be reused in Eskom. When a storage media is planned to leave Eskom, the simplest and most cost-effective method of sanitisation may be to destroy.

3.6 Control of storage media

A factor influencing Eskom sanitisation decision is who has control and access to the storage media. This aspect must be considered when the storage media leaves Eskom's control. The follow are examples of media control:

3.6.1 Under Eskom Control

Storage Media being turned for maintenance are still considered under Eskom control if contractual agreements are in place with Eskom and the maintenance provider with regards to confidentiality of information.

a) Maintenance being performed on Eskom's site, under Eskom supervision, by a maintenance provider where a non-disclosure agreement has been signed is also considered under the control of Eskom.

b) The storage media is being used within the business at another location.

3.6.2 Not Under Eskom Control

a) Storage media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to Eskom.

Therefore, storage media not under Eskom control shall be sanitised. It is recommended that storage media under Eskom control should still be sanitised if possible.

If equipment is removed off site as per 3rd party contract before sanitisation occurs and the equipment is not returned, a sanitisation certificate must be issued to Eskom by 3rd part. The sanitisation shall comply with this guideline.

4. Disposal

Once media storage and devices has been correctly sanitised by the appropriate destruction method (internally) and validated, a secure and appropriate method of disposal needs to be performed of the now classified e-waste. This will only relate to internal destruction methods as if destruction is done through and approved vendor, they would be responsible for the correct disposal method.

For internally destroyed media and with the adoption of the ISO 14001 standards within Eskom, recycling of the destroyed media is the preferred solution. Not only will this allow the business to reduce environmental impact as recycling of computer hardware is considered environmentally friendly because it prevents hazardous waste, including heavy metals and carcinogens, from entering the atmosphere, landfill or waterways but also allows the recovery of valuable rare earth metals and precious metals, which are in short supply.

Contracts and SLAs with approved and accredited electronic waste recycling services providers need to be utilised and the correct certificates and proof of recycling need to be obtained and stored along with the sanitisation documentation per item.

5. Sanitisation & Disposal per media type

All Destroy methods shall comply with the Eskom Waste Management Standard [4].

5.1 Hard Copy Storage

Table 1: Paper and microforms

Clear	N/A, see Destroy.
Purge	N/A, see Destroy.
Destroy	Destroy paper using crosscut shredders which produce particles that are 1 mm x 5 mm in size (or smaller) Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.
Dispose	Recycle the remaining components with an approved recycling vendor.

5.2 Networking Devices

Table 2: Routers and Switches (including modems)

Clear	Perform a full manufacture's reset of routers, switches or advanced modem/router back to its factory default settings.
Purge	N/A, see destroy.
Destroy	Disintegrate, Pulverize and Shredding the device or media storage core components
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.
Notes	Most networking devices contain removable storage. The removable media must be removed and sanitised using media-specific techniques.

5.3 Mobile Devices

Table 3: Mobile Devices

Clear	Manually delete all information, then perform a full manufacturer's/factory reset to reset the mobile device to factory state. Confirm any additional manufacturer specifications and clear options (e.g. IOS has full sanitise and BB has Security wipe) for factory reset and steps as per the user manuals. Sanitisation performed via a remote wipe should be treated as a clear operation.
Purge	If encryption is supported, perform a Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a purge capability that applies media dependent sanitisation techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.
Notes	Centralised management may be needed for encryption. Connect to power before starting encryption. Any additional storage media like SD cards will be sanitised by using the correct method for said media type.

5.4 Magnetic Media

Table 4: Floppies, Magnetic Disk (flexible or fixed), Reel & Cassette Format Magnetic Tapes, ATA & SCSI Hard Disk Drives

Clear	Overwrite media by using an Eskom approved tools. The clear pattern should be at least a single pass with a fixed data value, such as all zeros.
Purge	Overwrite method with a minimum of three total passes of a pseudorandom pattern (DoD Short) shall be written to the device.
Destroy	Shred, Disintegrate, Pulverize, or incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

5.5 Flash Based Storage Devices

Table 5: ATA Solid State Drives, SCSI Solid State Drives, NVM Express SSDs

Clear	Overwrite media by using an Eskom approved tools. The clear pattern should be at least a single pass with a fixed data value, such as all zeros.
Purge	Overwrite method with a minimum of three total passes of a pseudorandom pattern (DoD Short) shall be written to the device. If encryption is supported perform crypto/secure erase techniques using appropriate tools. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a purge capability that applies media dependent sanitisation techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Final alternative is Block erase method for SSDs. Select the appropriate one to perform with the tools available.
Destroy	Shred, Disintegrate, Pulverize or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

Table 6: Embedded Flash Memory on Boards and Devices

Clear	If supported by the device, reset the state to original factory settings.
Purge	N/A, see Destroy
Destroy	Shred, Disintegrate, Pulverize, and recycle/dispose the remaining components or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

5.6 Peripherally Attached Storage

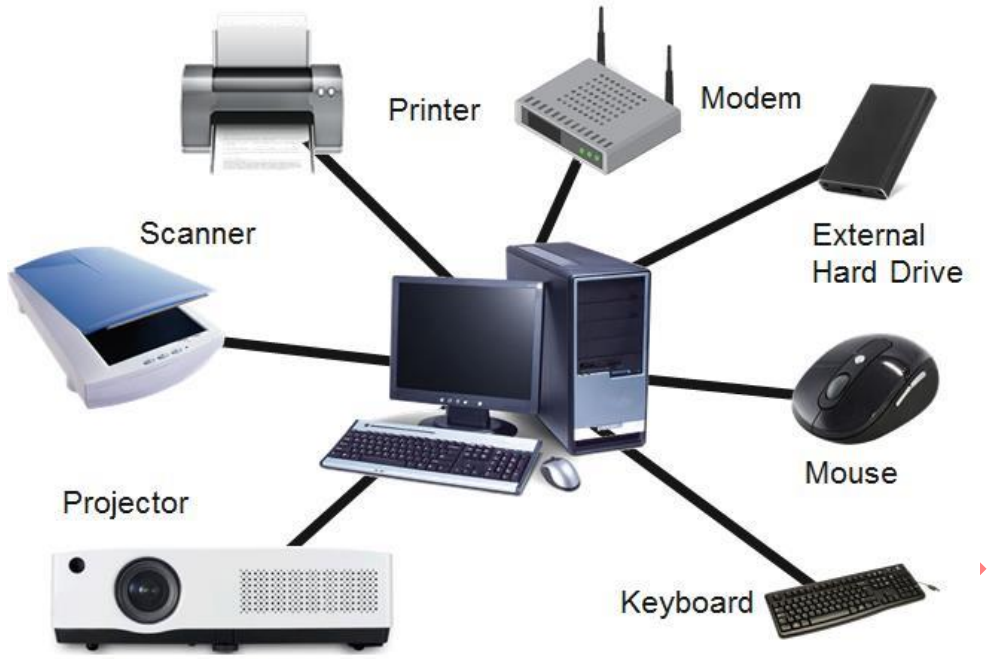

Figure 3: Examples of Peripheral Devices

Table 7: Externally Located Attached Hard Drives

Clear	Overwrite media by using an Eskom approved tools. The clear pattern should be at least a single pass with a fixed data value, such as all zeros.
Purge	Overwrite method with a minimum of three total passes of a pseudorandom pattern (DoD Short) shall be written to the device.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.
Notes	Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present.

Table 8: USB Removable Media & Memory Cards

Clear	Overwrite media by using an Eskom approved tools. The clear pattern should be at least a single pass with a fixed data value, such as all zeros.
Purge	Overwrite method with a minimum of three total passes of a pseudorandom pattern (DoD Short) shall be written to the device. If encryption is supported perform crypto/secure erase techniques using appropriate tools. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a purge capability that applies media dependent sanitisation techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Final alternative is Block erase method for SSDs. Select the appropriate one to perform with the tools available.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

Table 9: Office Equipment (copy, print, Fax machines)

Clear	Perform a full manufacture's reset and restore the office equipment to its factory default setting.
Purge	If encryption is supported, perform a Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a purge capability that applies media dependent sanitisation techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

5.7 Substation Equipment

Table 10: Substation Data Concentrators & RTU/Gateways

Note:	Sanitisation and disposal are only needed when the device will not be reused in the business. It has either reached end of life or is not functioning. The media storage component should be removed and sanitised appropriately and all remaining components can be disposed of as e-waste.
Clear	N/A
Purge	N/A
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

5.8 RAM and ROM-Based Storage Media

Table 11: Dynamic Random Access Memory

Clear	Power off device containing DRAM, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device.
Purge	Power off device containing DRAM, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Table 12: Electronically Alterable/Erasable Programmable Read-Only Memory (EAPROM & EEPROM)

Clear	Perform a full chip Purge as per manufacturer's data sheets.
Purge	Perform a full chip Purge as per manufacturer's data sheets.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

Table 13: Electronically Erasable Programmable Read-Only Memory (EEPROM)

Clear	Perform a full chip Purge as per manufacturer's data sheets.
Purge	Perform a full chip Purge as per manufacturer's data sheets.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the remaining components/e-waste with an approved recycling vendor or by another approved disposal method/provider.

5.9 Optical Media Sanitisation

Table 14: CD, DVD, BD

Clear	It a re-writable disk was used, overwrite media by using an Eskom approved tools. The clear pattern should be at least a single pass with a fixed data value, such as all zeros.
Purge	N/A, see Destroy.
Destroy	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Dispose	Recycle the material with an approved recycling vendor or by another approved disposal method/provider.

6. Verification

6.1 Verification of Equipment

Verification of the sanitisation process shall be done annually. If a sanitisation tool is used, such as a degausser, then the equipment calibrating, and equipment testing shall be verified.

6.2 Verification of Personnel Competencies

System Owners shall ensure the personnel conducting the sanitisation is competent to perform the sanitisation methods prescribed in this guideline. Consultation and guidance to be given to mechanical workshop personnel performing the sanitisation process to ensure the destruction is performed safely and to a standard of destruction that is adequate.

6.3 Verification of Sanitisation Results

Media shall be verified in two ways:

6.3.1 Full Read

For single or multiple media sanitisation verification, a full read of all accessible areas on the storage media shall be carried out to verify the expected sanitised values is in all addressable locations.

6.3.2 Representative Sampling

If multiple media are being sanitised and time and external factors do not permit a full read, then representative sampling can be done as such:

a) A pseudorandom location on each media each time is verified with an analysis tool.

b) Locations selected are over the full addressable space.

c) The size of each location shall be 5% of the total addressable space

d) The locations chosen must be non-overlapping

e) At least two non-overlapping locations shall be chosen for verification

f) Secondary verification shall be used on a subset of the media

6.4 Secondary Verification

Where representative sampling is used, secondary verification shall be used in addition to the process.

a) A subset of the media devices shall be full read verified.

b) The subset shall consist of a random chosen 20% of the media.

c) The verification shall be performed by an employee different from the representative sampling verification and with a different tool from the representative sampling verification.

d) If the secondary verification detects faults, all media in the set shall be re-sanitised.

Secondary verification provides assurance that the primary operation is working as expected.

7. Documentation

A certificate of media disposition shall be completed for each piece of electronic media that has been sanitised. A certificate of media disposition may be a piece of paper or an electronic record of the action taken. An example can be seen in Annex A.

All documentation shall be kept for a minimum period of 1 calendar year.

The certificate shall record the following:

a) Manufacturer

b) Model

c) Serial Number

d) Organisation Assigned Media

e) Media Type (magnetic, flash, hybrid, etc.)

f) Media Source (user or computer the media came from)

g) Pre-Sanitisation Confidentiality Level

h) Sanitisation Description (Clear, Purge or Destroy)

i) Method Used (degauss, overwrite, etc.)

j) Service provider information (Vendor or internal)

k) Work order issued or Contract information of vendor

l) Tools Used (including version)

m) Verification Method (full read or sampling)

n) Media destination (if known)

o) For sanitisation and validation:

   1) Name
   2) Position
   3) Date
   4) Location
   5) Contact number
   6) Unique number
   7) Signature

p) Data Backup Location (Optional – if data was backed up)

q) Disposal

   1) Method
   2) Contract number & Vendor Name (if used)

8. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Richard McCurrach	Senior Manager IM Tx
Christoph Kohlmeyer	Chief Engineer – Cyber security Gx
Malcolm Van Harte	Senior Manager Smart Grid Dx
Sithembile Songo	Senior Manager Information Security
Mervin Mottian	Middle Manager IM
Ezzard De Lange	Senior Manager – OT & IT Dx
Alison Maseko	Senior Manager – Eskom Telecomms
Comfort Masike	Senior Manager Technical Operations
Prudence Madiba	Senior Manager – Control and Instrumentation
Cornelius Naidoo	Middle Manager – Telecommunications Technology and Support
Beresford Jelliman	Chief Advisor IM Security
Mziwakhe Macina	Senior Advisor Cyber Security Dx
Rosalette Botha	Corporate Specialist – System Operator
Craig Boesack	Chief Engineer – Control and Instrumentation
Jorge Nunes	Chief Engineer – Control and Instrumentation
Zameka Qabaka	Senior Technologist – Koeberg Power Station
Ian Naicker	Chief Engineer – Control and Automation
Tsepo Thamae	Senior Advisor Cyber Security Tx

9. Revisions

Date	Rev.	Compiler	Remarks
June 2023	Draft 1.1	M Vala	Revision. Formalise the Certificate of Sanitisation to be used in the business and update document to include low cost, not contracted options for sanitization and disposal
Jan 2017	1	M Taljaard	New Document

10. Development team

The following people were involved in the development of this document:

- M Vala

11. Acknowledgements

Not applicable.

Annex A – Sanitisation form

Eskom

Certificate of Sanitisation		
PERSON PERFORMING SANITISATION		
Name:	Title:	
BU:	Location:	U/N:
MEDIA INFORMATION		
Make/Vendor:	Model Number:	
Serial Number:		
UID:		
Media Type:	Source:	
Data Classification level:	Data Backed up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITISATION DETAILS		
Sanitization Method Type: ☐ Clear ☐ Purge ☐ Destroy		
Sanitization Method used (Clear): ☐ Device Feature ☐ Software Tool ☐ Other:		
Sanitization Method used (Purge): ☐ Overwrite ☐ Block Erase ☐ Crypto/Secure erase ☐ Degauss (non-destructive) ☐ Other:		
Sanitization Method used (Destroy): ☐ Degauss ☐ Disintegration ☐ Pulverization ☐ Shredding ☐ Incineration ☐ Melting		
Sanitization Method details:		
Sanitisation Service Provider:		
Work order (internal) / Contract Number (external):		
Tools used (include version):		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Dispose ☐ Manufacturer ☐ Other (specify in details area)		
Details:		
Disposal information		
Method:		
Contract Number and Vendor details:		
SIGNATURE		
I attest that the information provided on this statement is accurate to the best of my knowledge:		
Signature:	Date	
VALIDATION		
Name:	Title	
BU:	Location:	U/N:
Signature:	Date	