Eskom	**Standard for Handling of Classified Items**	

Title: **Handling of Classified Items**

Document Identifier:	**32-143**
Alternative Reference Number:	**Not applicable**
Area of Applicability:	**Eskom Holdings SOC Ltd**
Functional Area:	**Security**
Revision:	**10**
Total Pages:	**21**
Next Review Date:	**December 2028**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Supported by	Functional Responsibility	Authorised by
Vhonani Mutswaletswale **Senior Advisor Vetting** **Group Investigations and Security**	**Romeo Malgas** **Middle Manager Vetting** **Group Investigations and Security**	**Botse Sikhwitshi** **Senior Manager Security Business Intelligence** **Group Investigations and Security**	**Peter Malitsha** **General Manager (Acting)** **Group Investigations and Security**
Date: 2025-11-25	Date: 2025-11-28	Date: 2025-11-28	Date: 2025-11-28

Content

Page

1. Introduction 3
2. Supporting Clauses 3
   - 2.1 Scope 3
     - 2.1.1 Purpose 3
     - 2.1.2 Applicability 4
     - 2.1.3 Effective date 4
   - 2.2 Normative/Informative References 4
     - 2.2.1 Normative 4
     - 2.2.2 Informative 5
   - 2.3 Definitions 6
   - 2.4 Abbreviations 8
   - 2.5 Roles and Responsibilities 8
     - 2.5.1 The HOD must: 8
     - 2.5.2 The Information Custodian must: 9
     - 2.5.3 The Information Owner (Originator) must: 9
     - 2.5.4 Eskom Vetting Fieldwork Unit 9
   - 2.6 Process for Monitoring 9
   - 2.7 Related/Supporting Documents 9
3. Procedure for Handling Classified Iterms 10
   - 3.1 Reason for Classification 10
   - 3.2 Non-Disclosure of Information 10
   - 3.3 Classification of Items 10
     - 3.3.1 Level of Classified Items 10
     - 3.3.2 General Rules Regarding Classified Items 10
   - 3.4 Drafting of Classified Information/Documents 12
   - 3.5 Identification of Classified Items 13
   - 3.6 Distribution 14
     - 3.6.1 Internal Circulation 14
     - 3.6.2 Printing of Classified Information 15
     - 3.6.3 External Circulation 15
   - 3.7 Removal of Classified Items from Premises 17
   - 3.8 Storing of Classified Information 17
   - 3.9 Destruction of Classified Items 19
   - 3.10 Loss of Classified Items 19
   - 3.11 Declassification and Reclassification of Classified Items 200
   - 3.12 Consequence of Negligent Loss of Classified Information 20
4. Acceptance 20
5. Revisions 21
6. Developmen Team 21

1. Introduction

As a state-owned entity, Eskom is required to protect sensitive and classified information in line with national laws such as the National Strategic Intelligence Act and the Minimum Information Security Standards (MISS). This standard aligns with MISS, the Eskom Security Vetting Policy, and other relevant legislation, including the Protection of Information Act, POPIA, and the Critical Infrastructure Protection Act.

Its purpose is to create a consistent framework for classifying, handling, storing, transmitting, and destroying classified items, ensuring the confidentiality, integrity, and availability of sensitive information. The standard promotes a security-conscious culture, holding employees and contractors responsible for safeguarding classified data.

Eskom staff and contractors must restrict access to sensitive information to those properly screened or vetted, applying the "need-to-know" principle and taking precautions against unauthorised access. Security measures must fully apply where disclosure exemptions exist, supplementing general business procedures and supporting good governance.

Classified information created or generated in hard copy or electronic format must be protected by implementing appropriate security measures. The content of the documentation determines the classification level and the level of protection for the document. This procedure must be used in conjunction with the Information Security Policy (32-85) with specific reference to Paragraph 2.2.5.

2. Supporting clauses

2.1 Scope

This standard applies to all classified information and assets handled by Eskom Holdings SOC Limited, its subsidiaries, and any other business entities in which Eskom maintains a controlling interest through capital or voting rights. It encompasses the processes of generating, receiving, altering, storing, dispatching, communicating, and archiving sensitive or classified information, whether in hard copy or electronic format, throughout the organisation’s operations.

The scope extends to all Eskom employees, contractors, temporary staff, subcontractors, vendors, business partners, and service providers, regardless of employment status or contractual arrangement. It covers all environments, including the nuclear sector, and mandates adherence to the minimum standards and guidelines outlined in this procedure for the secure handling, protection, and destruction of classified information and assets.

2.1.1 Purpose

To establish minimum standards and/or guidelines for the handling of classified information and/or items of Eskom Holdings SOC Limited, its subsidiaries and any other business entities in which Eskom has a controlling interest, either by its capital interests and/or voting rights.

As a custodian of national critical infrastructure, Eskom Holdings SOC Ltd is obligated to protect sensitive and classified information in accordance with national security legislation and standards, including the Minimum Information Security Standards (MISS) and the National Strategic Intelligence Act (Act No. 39 of 1994).

To establish a standard procedure that can be followed during the writing, compiling, receipt, dispatch, storage and destruction of classified items. The guidelines provided here are deemed necessary, but not limited to, if an applicable manager in their respective area wants to implement additional and stricter measures for the purpose of protecting any classified items, it can be done. No item will be generated, handled, stored or destroyed in a manner that may compromise any classified information and/or assets of Eskom.

This standard is developed in alignment with the Eskom Security Vetting Policy (32-0122M), the Information Security Policy (32-85), and applicable legislation such as the Protection of Information Act (Act No. 84 of 1982), the Protection of Personal Information Act (POPIA), and the Critical Infrastructure Protection Act (Act No. 8 of 2019).

These procedures apply to all Eskom employees, contractors, consultants, service providers, and any other individuals or entities involved in the generation, access, handling, or disposal of classified information or items within Eskom Holdings SOC Ltd and its subsidiaries.

The standard outlines a risk-based method for classifying and protecting information and assets, ensuring that security measures align with the sensitivity and potential consequences of compromise.

2.1.2 Applicability

This standard is applicable across Eskom Holdings SOC Limited, including all its divisions, subsidiaries, and any other business entities in which Eskom exercises control through capital investment, voting rights, or operational oversight. This includes, but is not limited to, the nuclear environment, strategic installations, and national key points as designated under applicable legislation.

The provisions of this standard apply to all Eskom employees (permanent, temporary, and contract), board members, interns, consultants, contractors, subcontractors, vendors, service providers, and business partners, regardless of employment status or contractual arrangement, who may generate, access, handle, store, transmit, or dispose of classified information or items.

Access to classified information and assets under this standard is determined by security vetting procedures, the need-to-know principle, and relevant Eskom and national security policies, such as the Eskom Security Vetting Policy and the Minimum Information Security Standards (MISS).

2.1.3 Effective date

This procedure will be effective from the date of approval.

2.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed below:

2.2.1 Normative

[1] Minimum Information Security Standards (MISS) [1996]

[2] 32-138: Vetting Administration Procedure.

[3] 32-85: Information Security Policy.

[4] 240-55410927: Cyber Security Standard for Operational Technology.

[5] 240-53716911: Overarching Group IT Policy.

[6] Private Security Industry Regulation (Act 56 of 2001) as amended.

[7] Critical Infrastructure Protection (Act 8 of 2019)

[8] Nuclear Energy (Act 46 of 1999)

[9] Regulation of Interception of Communications and Provision of Communications Related Information (Act 70 of 2002)

[10] Interception and Monitoring Prohibition (Act of 1995)

[11] Electronic Communications and Transactions (Act 25 of 2002)

[12] Electronic Communication (Act 68 of 2002)

[13] National Strategic Intelligence (Act 39 of 1994)

[14] Prevention of Organised Crime (Act 121 of 1998)

[15] Protected Disclosures (Act 26 of 2000)

[16] Protection of Information (Act 84 of 1982)

[17] Protection of Personal Information (Act 4 of 2013)

[18] Promotion of Access to Information (Act 2 of 2000)

[19] Public Finance Management (Act 1 of 1999)

[20] Minimum Physical Security Standards (MPSS) [2015]

[21] 32-0122M Security Vetting Policy.

2.2.2 Informative

[21] ISO 9001:2015 Quality Management System Standards.

[22] 32-86: Integrated Risk Management Policy.

2.3 Definitions

Definition	Explanation
Author	The person who prepares, compiles, generates, or initially classifies a document.
Classification	All official matters requiring the application of security measures (excepted from disclosure) must be classified **"Confidential", "Secret" or "Top Secret".**
Classified Information	Sensitive information which is in the national interest of the Republic of South Africa, is held by, is produced in or is under the control of Eskom Holdings SOC Limited, or which concerns Eskom Holdings SOC Limited, and which shall, because of its sensitive nature, be exempted from disclosure and must be protected against any threat and/or where information and/or assets can be compromised in any way.
Classified Item	An item that forms part of, or contains, classified information
Classify and/or reclassify	With reference to MISS. The grading and/or arrangement or re-grading / re-arrangement of any information in any format, in accordance with its sensitive (level of classification) or in compliance with the set minimum security requirements
Communication Security	That condition is created by the conscious provision and application of security measures for the protection of classified communication.
Compromise	The authorised disclosure/exposure of loss of sensitive or classified items (information and/or assets), or exposure of sensitive operations, people and/or places, whether by design or through negligence
Confidential	The classification awarded to information that may be used by malicious/opposing/hostile elements to **harm** the objectives and functions of Eskom Holdings SOC Limited, its subsidiaries and any other business entities in which Eskom has a controlling interest, either by its capital interests and/or voting rights.
Control Register	The register containing all classified items handled by an appropriate office
Controlled Disclosure/Declassification of Documents	The way classified information is declassified to be disclosed with appropriate consent and to authorised persons
Copying/Duplicating/Reproducing	Making a copy of any document, whether copying it out by hand, reproducing it by photographic or any other means
Declaration of Secrecy	An undertaking by a person who has had, currently has, or will have access to classified information, that he/she will treat such information.

Definition	Explanation
Destruction of Classified Material	The doing away with/expunging or destroying of classified documents/articles/equipment in any form.
Document	In terms of the Protection of Information (Act 84 of 1982), a document is: • Any note or writing, whether produced by hand or by printing, typewriting or any other similar process. • Any copy, plan, picture, sketch or photographic or other representation of any place or article. • Any disc, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction.
Document Register	A register (digital or physical) kept by the head of department in which all documents are recorded.
Eskom *(Eskom Holdings SOC Limited)*	Eskom Holdings SOC Limited, its subsidiaries and any other business entities in which Eskom has a controlling interest, either by its capital interests and/or voting rights.
HOD	The head of the department who is authorised to handle or who stores it.
HOI	The person who is serving as the Head of an Institution, whether defined by law or otherwise, including the official acting in his place.
Information Custodian	A user or legal entity that is responsible and/or accountable for implementing the necessary control measures to protect the information and the information resources as per the level of classification awarded by the owner and/or by any applicable law.
Information Owner	A user or legal entity who creates or initiates the creation or storage of the information is the initial owner. The owner is responsible for assigning a classification to the information and dictating how the information should be handled and/or protected.
Line Manager	The direct responsible manager of an employee.
Need-To-Know Principle	The furnishing of only that classified information or part thereof that will enable a person (s) to carry out his/her task.
Secret	The classification awarded to information that may be used by malicious/opposing/hostile elements to **disrupt** the objectives and functions of Eskom Holdings SOC Limited, its subsidiaries and any other business entities in which Eskom has a controlling interest, either by its capital interests and/or voting rights.
Security Clearance	An official document issued by the Director-General of the State Security Agency (Domestic Branch) [SSADB] indicating the degree of a person's security competence.

Definition	Explanation
Security Screening/ Security Vetting	The systematic process of investigation is followed in determining a person's security competence.
Top Secret	The classification awarded to information that may be used by malicious/opposing/hostile elements to **neutralise** the objectives and functions of Eskom Holdings SOC Limited, its subsidiaries and any other business entities in which Eskom has a controlling interest, either by its capital interests and/or voting rights.

2.4 Abbreviations

Abbreviation	Explanation
BU	Business Unit.
DoS	Declaration of Secrecy
VFU	Vetting Fieldwork Unit.
GCE	Group Chief Executive (Eskom Holdings SOC Ltd)
GIS	Group Investigations and Security
HOD	Head of Department in Eskom.
NDA	Non-Disclosure Agreement.
NDI	Non-Disclosure of Information.
SOC Ltd	State Owned Company Limited.
SSA	State Security Agency.

2.5 Roles and Responsibilities

2.5.1 The HOD must:

a) Determine which job positions within the department may be exposed to classified information.

b) Ascertain the appropriate classification level for such information (as outlined in Section 3.2).

c) Inform the relevant incumbent about the classification determination.

d) Ensure that all incumbents are vetted to the required level in accordance with MISS requirements and Eskom's vetting policy.

e) Ensure all incumbents are aware of and comply with these requirements and maintain a control register.

f) Ensure proper classification of departmental documents and information in line with the MISS and Eskom Information Security Policy and periodically review classifications to avoid under- or over-classification.

g) Maintain oversight of access control mechanisms, ensuring that only authorised and vetted personnel have access to classified items, and that the need-to-know principle is strictly enforced.

h) Report any breaches, losses, or suspected compromises of classified information to Group Investigations and Security (GIS) and the State Security Agency (SSA) within the prescribed timeframes.

i) Ensure contingency plans are in place for the protection and destruction of classified items during emergencies, in accordance with Eskom's Business Continuity and Risk Management frameworks.

j) Conduct regular audits and inspections of classified item handling practices to ensure compliance with this standard and to identify areas for improvement.

k) Ensure that all classified items are recorded, tracked, and stored securely, and that the control register is consistently updated and reconciled.

2.5.2 The Information Custodian must:

Ensure that the necessary safeguards and controls are implemented to protect the classified item as per classification by the originator and/or information owner.

2.5.3 The Information Owner (Originator) must:

Classify their information to the relevant security classification level, review and maintain all classified information and/or items regularly.

2.5.4 Eskom Vetting Fieldwork Unit:

a) Facilitate security awareness and training programmes for employees throughout the business (Divisions, subsidiaries and departments) regarding the handling, storage, transmission, and destruction of classified information.

a) Monitor compliance throughout the business (Divisions, subsidiaries and departments) and recommend corrective action.

2.6 Process for Monitoring

As prescribed within the adopted quality management system (ISO 9001:2015) of Eskom Holdings SOC Limited, regarding the handling and/or storing/archiving of records and documentation.

2.7 Related/Supporting Documents

Please refer to 2.2. Narrative/Informative References of this Standard (32-143 Handling of Classified Items).

3. Procedure for Handling Classified Items

3.1 Reason for Classification

Items are classified to ensure that Eskom's efficient functioning is not impaired by persons using sensitive information to the detriment of the organisation, South Africa, or the South African government.

All Eskom staff exposed to classified items must be dually vetted by the Eskom Vetting Fieldwork Unit/SSA and need to sign a Declaration of Secrecy (DoS) as prescribed by the MISS document.

3.2 Non-Disclosure of Information

No person, employed by Eskom on a permanent or contract basis, will disclose any classified information related to Eskom to anyone without the authorisation of the HOD/line manager of such employee. All disclosures external to Eskom are prohibited unless authorised by the GM Security.

3.3 Classification of Items

3.3.1 Levels of Classified Item

a) **Top Secret:** This classification is reserved for information of an extremely sensitive nature, technical, intellectual, commercial, or financial, where unauthorised disclosure could neutralise Eskom's strategic objectives, severely damage national interests, or result in catastrophic operational failure. Only individuals with a valid Top Secret security clearance may classify or access such information. Circulation must be strictly limited and controlled under the highest security protocols.

b) **Secret:** This classification applies to information that, if disclosed, could disrupt Eskom's operations, **compromise** strategic plans, or damage relationships with contractors, stakeholders, or government entities. Only individuals with a Secret or higher clearance may classify or access such information. Circulation must be restricted and monitored.

c) **Confidential:** This classification covers information that, if shared, could harm Eskom's reputation, operations, or finances. Examples include internal messages, personnel issues, and sensitive business data. Only those with Confidential clearance or higher may access it, in accordance with the need-to-know principle.

d) **Restricted:** Restricted information describes material that, if disclosed, could result in inconvenience or minor disruption to operations. Such information necessitates basic protective measures and restricted access, but does not meet the criteria for higher security classifications.

3.3.2 General Rules Regarding Classified Items

a) No Eskom employee(s) or contractors/consultants' employee(s) employed by Eskom shall be provided or entrusted with sensitive/classified information before the person or company is security screened and/or vetted to the appropriate level.

b) Eskom employee(s) or contractors/consultants' employee(s) employed by Eskom shall not disclose any official Eskom information or documentation to a third party without the written consent and authorisation of the HOD/author.

c) The classification of an item (document) will be determined by the content or the importance of such, and the highest classification grade/level will be allocated. The same classification as that of the original shall be assigned to any extracts from that document/item.

d) Every document shall be classified on its own merits by the original author and not in accordance with its connection to some other classified document.

e) Based on the minimum information security standards (MISS), a document written in reply to a classified document received from outside Eskom shall bear the same minimum classification as the incoming document.

f) When the State Security Agency (Domestic Branch) declares that an employee cannot obtain a security clearance for whatever reason, and he/she must have access to classified items, the GCE will take full responsibility for such a person. It is recommended that such a person be moved to an area where no classified or sensitive information is handled or used.

g) All employees, contractors, and consultants must sign a Declaration of Secrecy (DoS) before commencing duties involving access to classified information. The declaration must be explained to the individual, retained in their personnel file, and reaffirmed periodically as part of ongoing security awareness.

h) All classified items must be reviewed periodically to determine whether the classification remains appropriate. Reclassification or declassification must be conducted in accordance with MISS and Eskom's internal procedures.

i) Only authorised personnel with the requisite security clearance may assign, change, or approve the classification level of documents or items. This authority must be documented and monitored by Group Investigations and Security (GIS).

k) When a document or item contains information of varying classification levels, the highest applicable classification shall be assigned to the entire item unless otherwise authorised by the information owner.

l) Classified items must be stored and transmitted using approved methods and infrastructure, including encrypted digital platforms and secure physical containers, as prescribed by Eskom's Information Security Policy and MISS.

m) Access to classified items must be logged and monitored. Audit trails must be maintained to ensure accountability and traceability of all interactions with classified information.

n) All personnel handling classified items must undergo mandatory security awareness training, including refresher courses, to ensure understanding of classification protocols and responsibilities.

o) Any suspected or confirmed breach, compromise, or unauthorised disclosure of classified items must be reported immediately to Group Investigations and Security (GIS) and the State Security Agency (SSA), in line with Eskom's incident response procedures.

p) External service providers, vendors, and contractors must be contractually bound to comply with Eskom's classification and information protection standards, including signing non-disclosure agreements (NDAs) and undergoing vetting.

3.4 Drafting of Classified Information/Documents

a) Items in semi-completed or draft form shall be kept in a safe place (see Paragraph 7) when they are not being worked on.

b) Precautions shall be taken to dispose properly of all aids used in drafting classified items so that such aids do not constitute a security risk. Drafts, notes, rough or detailed sketches, photographs, voice or video recordings, and computer-based presentations have to be stored separately in the prescribed manner (depending on classification), under lock and key, and periodically collected by an officer designated to do so and destroyed by burning or shredding. Computer-generated draft material shall be stored in secure and/or encrypted media.

c) The author of a classified document shall indicate thereon whether it may be reclassified/declassified after a certain period or upon the occurrence of a particular event. This option must be applied consistently for documents with a classification of "Confidential" or higher.

d) Where the recipient of a classified document believes that such a document should be reclassified, he/she must obtain written authorisation from the author, the head of the department or his/her delegate(s) for this purpose.

e) All **"Top Secret"** and **"Secret"** items shall not be copied or reproduced and will remain in the original format. All "Top Secret" and "Secret" documents must include copy numbers.

f) Only typists/secretaries who have the necessary clearance may type or have access to classified documents/items. Temporary or stand-in typists/secretaries who have not been cleared to the required level, but need to have *ad hoc* access to classified items, shall sign a Declaration of Secrecy (DoS).

g) Classified files should be opened only when an actual need arises due to the sensitivity of the content, not merely because the filing system provides for the existence of such a file. ***(Beware of under- and over-classification).***

h) The particulars appearing on classified files should include at least: the name/topic of the file, the file number, the classification and the names of the person/persons who is/are authorised to have access to that file, document number and copy number where applicable.

i) A register shall be kept of all classified files opened/in existence. As and when a file is opened, the particulars must be entered in the register. The register itself will be classified to at least the "Confidential" level.

j) All documents in a classified file shall be given a serial or index number, in the sequence in which each document is filed, but preferably in chronological order. The file will be assigned the classification of the highest-classified document within it.

k) A sub-file shall be opened for each file and kept inside the main file. Each sub-file shall have the same particulars as the main file. When the main file is removed from the room where such files are kept (which should not be common practice), an entry must be made on the sub-file indicating to whom and when the main file was issued. This must also be registered in a document removal register, and the custodian must ensure that the file is handed back before the end of business on the particular day for safekeeping.

l) No file is allowed to remain outside the dedicated room for longer than one working day. Classified files shall always be stored in a lockable reinforced steel cabinet when not in use, outside the dedicated space.

m) Only authorised persons may be allowed access to classified files. Internal policy should dictate who may authorise such access, subject to the need-to-know principle.

n) All draft versions of classified documents must be clearly marked as “DRAFT” and include version numbers, authorship, and date of creation. A version control register should be maintained to track changes and ensure accountability.

o) Digital drafts must be stored in secure, access-controlled environments with encryption. Metadata associated with classified documents (e.g., author, timestamps, revision history) must be protected to prevent unauthorised inference or compromise.

p) Collaboration on classified drafts must be conducted using Eskom-approved secure platforms that support encryption, access control, and audit logging. Use of personal devices or unauthorised cloud services is strictly prohibited.

q) Temporary digital files, cached data, and auto-saved versions of classified drafts must be securely deleted using Eskom’s approved data sanitisation tools and procedures.

3.5 Identification of Classified Items

a) The classification assigned to an item shall be typed/printed or stamped at the top and bottom (preferably in the middle) of each page (loose or bound) and on the cover.

b) Tracings or blueprints shall be marked in such a way that the classification is visible on all copies. If this is not possible, rubber stamps should be used to mark all copies.

c) Where it is physically impossible to mark an item clearly, for example, tape recordings, certain photographs and negatives, the item shall be placed in a suitable box, envelope or other container and, if necessary, sealed. The nature and classification of the contents shall be clearly marked on the outside of the container.

d) Classified items shall be marked in such a way that the mark is clearly visible, even when the items are rolled or folded. However, care should be taken not to obliterate important details and to ensure that the marking cannot be removed or altered unobtrusively.

e) When items are filed together, the cover shall bear the mark of the items with the highest classification. However, items with a different classification should, as far as possible, be filed in different files/volumes.

f) The mark or stamp shall comply with the prescribed organisational standard, as indicated in the MISS document.

g) Where feasible, colour-coded stamps or borders may be used to visually distinguish between classification levels (e.g., red for Top Secret, blue for Secret, green for Confidential, yellow for Restricted), in accordance with Eskom’s approved marking standards.

h) For electronic documents, classification markings must be embedded in the header and footer of each page, and metadata must reflect the classification level. Watermarks may be used to reinforce visibility. Classification must also be reflected in the document properties and file name.

i) All printed classified documents must include a cover sheet indicating the classification level, handling instructions, and distribution restrictions. The cover sheet must be securely attached and marked in accordance with organisational standards.

j) Any annexures, appendices, or attachments to a classified document must be individually marked with the appropriate classification level. If the annexure contains information of a higher classification than the main document, the entire document classification must be upgraded accordingly.

k) USB drives, CDs, DVDs, and other removable media containing classified information must be physically labelled with the classification level and securely stored. Digital labelling must also be applied to the file system.

l) Emails, instant messages, and other digital communications containing classified information must include classification markings in the subject line and body text and must be transmitted only via approved secure channels.

m) Classification markings must be reviewed periodically to ensure consistency, accuracy, and compliance with Eskom and MISS standards. Any discrepancies must be reported to Group Investigations and Security (GIS) for corrective action.

3.6 Distribution

Classified information may only be disclosed to authorised persons with a valid security clearance, and additional restrictions of the **"NEED-TO-KNOW Principle"** will need to be applied. Access to the classified material must be restricted to the minimum.

Copies

a) Where possible, if extracts rather than copies are made (preferred) of classified documents/items, the same classification level of the original document will need to apply.

b) Copies and extracts of classified information shall be made only after obtaining **authorisation from the author/authorised HOD,** therefore from the compiler, the addressee or such other senior person as may usually have access to those items.

c) No copies/extracts of **Top Secret** and **Secret classified documents and** items shall be allowed.

3.6.1 Internal circulation

a) All Secret/Top Secret classified items to be circulated internally (within the same locality/building) shall be taken to the addressee personally by a specifically designated person who, in turn, has to have a security clearance and may not be circulated by internal mail. The documents shall be sealed in the double envelopes as prescribed and must be signed for by the receiver in a document register.

b) In the case of classified Eskom publications, the provision of the Standard for Reference Libraries IS/ SI, paragraph 2.5.1, which stipulates that those three (3) copies of internal

publications shall be dispatched to the central library, need not be observed. It will suffice if copies of the title page and table of contents are sent to the library, archive or stored on the designated document management system for indexing, as well as an indication of where the document is available.

3.6.2 Printing of Classified Information

a) All classified internal documents must only be printed via a printer equipped with password protection.

b) All printers to archive/delete unprinted classified information within 24 hours.

3.6.3 External Circulation

a) Receipt and distribution of documents

- The responsible manager shall appoint a person to be responsible for the receiving, recording and distribution of all classified items.
- All incoming classified items shall be received, stamped with an office stamp and registered by appropriately cleared staff. The object of such registration is to exercise total control over these classified documents.
- The above-mentioned items shall, without opening the inner envelope, be handed over to the addressee, or to appropriate officials who are authorised to open items in a certain category.
- All classified Confidential, **Top Secret** or **Secret** items which are dispatched, made available or distributed shall be registered to ensure control.
- When **Confidential**, **Top Secret** or **Secret** documents are dispatched, made available or distributed, the addressee is required to give a written acknowledgement of receipt. The recipient also needs to produce a form of identification in order for the courier to determine if it is the correct person receiving the document. Such acknowledgement of received documents will, in turn, be kept in a secure location and will be stored digitally on the document management system.

b) Preparation for dispatch

- All classified items have to be correctly prepared for dispatch that includes serial number of entry, date of dispatch, reference of document, date of document, classification of document, subject/heading, dispatched/addressed to, nature of dispatch *(courier by hand, registered post, facsimile or computer)*, registered number of postal material, signature of the recipient *(courier, registration person dispatching)*, receipt number and date when receipt was obtained. The classification and heading of the document must be placed in the inner envelope so they are not visible from the outside.
- Any deviation from this procedure may be considered suspicious and eligible to be investigated as a possible breach of security.

c) Standard procedure for dispatch:

- Place the information item in a new envelope, seal it and address it. Then stamp the security classification on the front and sign across the envelope flaps. Envelopes marked Confidential during printing may also be used.

- The seals of the inside envelope shall be properly sealed by paper seals, countersigned and have the name of the office of origin clearly stamped on them. After that, broad translucent tape shall be placed on the seams, covering the seals and the stamps.
- The reference number of the document, the name and address of the addressee and other special instructions for dealing with the document shall be entered clearly on the front of the inner envelope.
- In the case of **Top-Secret** matters, the envelope shall have entered on it a clear indication as to who may open it, e.g., "to be opened by _____ (name) only".
- The sender's name and address shall be written on the back of the envelope so that the item may be returned, if necessary, without opening it.
- Under no circumstances may an indication of the nature or classification of the contents appear on the outer envelope since this could attract unwanted attention.
- Then the sealed and stamped envelope is placed inside another, unmarked, outer envelope, which shall be addressed appropriately. A receipt to be signed by the recipient and returned to the sender must be attached to the document and placed inside the outer envelope. It is therefore clear that classified items are sent within two envelopes, an inner and an outer envelope.

d) Means of dispatch (refer to 3.5.3.2 a) as per MISS

- Confidential items could be sent by registered post, courier or by hand.
- Secret items may only be sent and delivered by hand.
- Top Secret items may only be sent and delivered by hand (using suitably cleared employees).
- Top Secret items shall be noted in a register indicating the title/description of the item and the time and date of dispatch and may only be handed over to the employee/courier upon obtaining a signature.
- A courier may only convey classified items in a secure locked container, and it is recommended that the container be equipped with a high security or combination lock.
- Couriers shall have at least a *"Confidential"* security clearance and, wherever possible, be accompanied by a second person.
- The courier must obtain an appropriate receipt for the items from the addressee.
- Upon the return of the courier, a responsible officer shall check the receipts obtained for classified items.
- Control must be exercised over the time taken by a courier to deliver the documents. Upon receipt, the recipient must check that the items have not been compromised.
- Couriers must be able to identify themselves by photo identification when fetching or dispatching post.
- When **Top Secret** and **Secret** items are dispatched, the sender is obliged to ascertain whether the document has in fact reached the addressee. An acknowledgement of receipt should be included for the receiver to sign and return to the sender.

e) Dispatch by means of facsimile:

- When classified documents are transmitted by means of facsimile, only cryptographically protected facsimile machines approved by State Security may be used between the sender and the recipient.
- A record shall be kept of the dispatch and receipt of classified documents.
- The sender shall notify the receiver before dispatch of the classification, reference, date, and title, number of pages and serial number of the documents concerned.
- The receiver shall, upon receipt of the documents, ascertain whether they are clear, accurate and complete. Then, an acknowledgement of receipt shall be sent to the sender.
- The recipient shall enter the copy number as indicated on the distribution list on his/her copy.

f) Computerised dispatch of documents

- When classified (Secret/Top Secret) documents are forwarded by computer, appropriate **line protection** shall be ensured. Information security controls shall be used, such as encryption and digital certification, as prescribed by the organisational information security policy.
- All magnetic media shall be regarded as documents and handled as such.
- All classified items transmitted and received by computer shall be recorded, and the recipient shall acknowledge receipt.

Note: *Dispatch by facsimile or computer should be limited to the most exceptional cases only.*

3.7 Removal of Classified Items from Premises

a) The removal of classified items from office buildings shall be prohibited unless for business purposes and with the necessary approval.

b) Classified (Secret/Top Secret) items may not be taken home unless proper lock-up facilities exist there, and such removal of classified items must be approved in writing by the head of the department or his/her duly authorised delegate.

c) Classified items taken to a meeting outside the building in which they are normally kept shall be carried in a lockable security attaché case, and great care shall be exercised to avoid compromising the contents.

3.8 Storing of Classified Information

a) When classified documents are not in use, they must be stored in the following way:

- **"Confidential":** Reinforced lockable filing cabinet.
- **"Secret":** Strong room or reinforced lockable fireproof filing cabinet within a security-controlled area. Electronic documentation should be stored and encrypted with a password and kept separate from a personal computer.

- **"Top Secret":** Strong room, safe or walk-in safe within a security-controlled area. Electronic documentation should be stored and encrypted with a password and kept separate from a personal computer.
- **Classified** items **may not**, under any circumstances, be left unattended.

b) The doors of all offices in which classified items are kept shall be equipped at least with high security locks. The keys to a room, safe-deposit, or cabinet in which classified items are stored will not be allowed. Effective key control must be properly maintained and effectively exercised. Duplicate keys and the codes of combination locks shall be kept in a sealed envelope by the head of Security/key custodian, and combination codes should be changed as per the MISS recommendation.

c) The combinations of the combination locks of a strong room or safe shall be changed every three months and in the following circumstances:

- When it is suspected that a combination may have been compromised.
- When a new user assumes responsibility, and
- When the responsible person resumes duty after a prolonged absence, and the code has necessarily been disclosed to another person.
- No unauthorised person may be present when the new combination is set, or the lock is opened.

d) Proper access and movement control inside any building or part of a building in which classified items are handled must be ensured and enforced.

e) Where necessary, the doors, windows, fanlights, passages, stairs, etc., giving access to the room where classified items are kept, should be equipped with locks, bolts, and iron bars; all of adequate strength.

f) Apart from the above, all the doors of a room where classified items are handled shall be fitted with solid wooden doors, high security locks, door closures and be kept locked when the room is vacated, even for a short while. If the responsible person leaves the room for a longer period, e.g. at lunchtime, all Secret and Top-Secret items shall be locked away in a safe or a metal cabinet of adequate strength equipped with a security lock.

g) Access to any controlled building, part of a building or room where classified items are handled or stored outside normal office hours should be prohibited to all persons. Access to the area will only be granted by security if authorisation from the departmental head is obtained. Repairs to and the cleaning of such controlled building, part of a building or a room shall take place in the presence and under the supervision of the persons who work there during operational hours. Persons who must gain access to such a building after hours should be duly authorised by the head of the department or his/her delegate.

h) No classified item may be stored off-site or outside the control of Eskom, unless authorised by the author/HOD/line manager or summoned by the local law enforcement authorities.

3.9 Destruction of Classified Items

a) Classified items may only be destroyed on the instruction of the compiler and/or in accordance with the Eskom and National Archive of South Africa prescribes. The retention period for different types of documents differs; therefore, ESKOM and the National Archives of South Africa prescribe, and the recommendation needs to be implemented/adhered to.

b) Where destruction has appropriately been authorised by the HOD, it should take place by burning or some other approved method, e.g. shredding (by means of a crosscut machine), in which case the strips may be no wider than 1,5 mm. The responsible person who destroyed the items shall provide the head of the department with a certificate of destruction for the items concerned.

c) The process of destruction shall eliminate all possibility of reconstructing the item.

d) In the case of the destruction of items from another department, a destruction certificate shall be supplied to the author.

e) The contingency plan of a department must make provision for the destruction, storage and/or moving of classified items in the event of an emergency, to prevent the risk of items being compromised. The possibility of off-site storage with a reputable firm must be reported to Security for investigation.

f) The destruction of classified items in electronic or soft copy format needs to comply with the standards and procedures set by the Group IT Division.

3.10 Loss of Classified Items

a) The loss of any Eskom-issued laptop must be reported to the Security Department within 24 hours, who, in turn, must ensure the loss of the laptop is reported to the State Security Agency (SSA) and the Eskom Vetting Fieldwork Unit (VFU).

b) If **confidential** items are lost, the compiler shall be notified immediately. The person responsible for the documents shall take all reasonable steps to recover them and to prevent a recurrence.

c) If **Top Secret** and/or **Secret** documents are lost, the managers and general managers of the department where such documents were lost and of the department where they were compiled shall be notified immediately upon discovery of such loss, and a full investigation must be initiated.

d) If a breach of security occurs or when classified documents become lost, the general manager/BU manager concerned will request a confidential investigation, and the incident will need to be reported to SSA within 24 hours.

If necessary, a board of inquiry consisting of a representative from the organisation segment where the document was lost, a representative from the Security Division, Audit & Forensic and Legal Departments or any other persons nominated by the persons referred to in Paragraph 3.9.2, may be convened to take the necessary action.

3.11 Declassification and Reclassification of Classified Items

a) Under classification and overclassification: The author of a document must guard against the under classification, overclassification or unnecessary classification of documents.

b) Reclassification: When the author of a classified document indicates thereon whether it may be reclassified after a certain period or upon the occurrence of a particular event. This option is to be applied consistently upon the award of a classification. A security classification needs to be reviewed due to changed circumstances. Only the author of the document shall re-classify the document to a lower level of classification and notify all persons.

c) Retention period of classified items for declassifying/classified items or reclassifying previously classified or new items must comply with the minimum storage period set by any legislation applicable to those classified items.

3.12 Consequences of Negligent Loss of Classified Information

a) The loss of classified information through negligence, including laptop theft, will be dealt with in accordance with the Eskom Code of Conduct.

b) The loss of an Eskom-issued laptop will also be dealt with under 3.12 (a).

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Peter Malitsha	General-Manager: Group Investigations and Security (Acting)
Botse Sikhwitshi	Senior Manager: Security Business Intelligence
Nomsa Spaumer	Senior Manager: Security Business Enablement
Remone Govender	Senior Manager: Forensic and Anti-Corruption (Acting)
Anusha Govender	Middle Manager: Security Investigations
Romeo Malgas	Middle Manager: Vetting
Wayne Cairns	Senior Manager: Security Solutions (Acting)
Samaria Mabona	Middle Manager: Eskom Real Estate
Monette Heath	Middle Manager: Generation Security
Melvin Murugen	Middle Manager: NTCSA
Adolph Lekganyane	Middle Manager: Distribution
Motlhatlhani Khunou	Middle Manager: Security Risk Management
Ishana Narotam Bhoola	Middle Manager: Information Solutions

5. Revisions

Date	Rev.	Compiler	Remarks
November 2025	10	RJ Malgas	Reviewed and updated the Standard.
March 2017	9	P Malitsha	Reviewed and updated the Standard.
November 2016	8	R Dreyer	Reviewed and updated the Standard.
September 2016	7	R Dreyer	Reviewed and updated the Standard.
September 2016	6	P Malitsha	Reviewed, Updated - Converted to a Standard.
March 2016	5	LP Human	Reviewed and updated the Procedure.
April 2014	4	A Govender	Reviewed and updated the Procedure.
October 2010	3	PJ Fouche	Reviewed and updated the Procedure.
February 2008	2	PJ Fouche	Revised, Updated - Converted to a Procedure.
December 2003	1	PJ Fouche	Added Reference ESKADABT3

6. Development Team

This document originated from an integrated team within the Group Investigations and Security and was revised by Security Business Intelligence.

- Romeo Malgas
- Vhonani Mutswaletswale