	Standard	
---	-----------------	--

Title: **Handling of Classified Items**

Document Identifier: **32-143**

Alternative Reference Number: **Not applicable**

Area of Applicability: **Eskom Holdings SOC Ltd**

Functional Area: **Security Division**

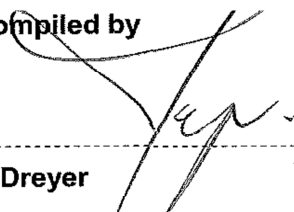
Revision: **9**

Total Pages: **15**

Next Review Date: **November 2021**


Disclosure Classification: **Controlled Disclosure**

Compiled by


 R Dreyer
 Senior Advisor SBI
 Security Division

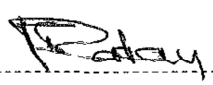
Date: 2017-01-09

Functional Responsibility


 L P Human
 Middle Manager SBI
 Security Division

Date: 2017-01-09

Authorized by


 TJ Rakau
 Divisional Executive
 Security Division

Date: 2017-01-12

Content

	Page
1. Introduction.....	3
2. Supporting Clauses	3
2.1 Scope.....	3
2.1.1 Purpose.....	3
2.1.2 Applicability	3
2.1.3 Effective date.....	3
2.2 Normative/Informative References	3
2.2.1 Normative.....	3
2.2.2 Informative.....	4
2.3 Definitions	4
2.4 Abbreviations	5
2.5 Roles and Responsibilities	6
2.5.1 The HOD must	6
2.5.2 The Originator of the document must.....	6
2.6 Process for Monitoring.....	6
2.7 Related/Supporting Documents.....	6
3. Procedure for Handling Classified Items.....	7
3.1 Reason for classification.....	7
3.2 Non-Disclosure of Information	7
3.3 Classification of items.....	7
3.4 Drafting of classified information/ documents	8
3.5 Marking of classified items	9
3.6 Distribution	9
3.7 Removal of classified items from premises.....	12
3.8 Storing of classified information.....	12
3.9 Destruction of classified items	13
3.10 Loss of classified items.....	13
3.11 Declassification and Reclassification of classified items	14
4. Acceptance.....	14
5. Revisions.....	15
6. Development Team	15
7. Acknowledgements	15

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

1. Introduction

Eskom employees and contractors generate, receive, alter, store, dispatch, communicate and archive sensitive information by means of various methods during the course of business. Access to sensitive information and assets must be limited to persons who are appropriately reliability screened/ security cleared and who have a "need-to-know". Precautions must be taken to ensure that persons that are not cleared, who may be in the proximity of information and assets, do not gain access to this information and assets.

Sensitive information is created in hard or electronic form must be protected by implementing the necessary security measures. The degree of sensitivity determines the level of protection that is required. 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

2.1.1 Purpose

To establish a standard procedure that can be followed during the writing, the compiling, the receipt, the dispatch and the storage of classified items. The guidelines provided here do not exclude the specific instructions given by any manager, which means that when departmental heads are of the opinion that stricter or more specific measures are necessary, such measures will apply. No item will be generated, handled or stored in a manner that may compromise any classified information contained therein.

2.1.2 Applicability

This procedure shall apply throughout Eskom and its subsidiaries Holdings SOC Ltd divisions and any other business entities in which Eskom has a controlling interest, either by its capital interest and/ or voting rights.

2.1.3 Effective date

This procedure will be effective from date of authorisation.

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

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- [2] 32-85 Information Security Policy
- [3] ISO 9001:2015: Quality Management System Standards
- [4] Act 84 of 1982: Protection of Information Act, Section 4
- [5] Act 39 of 1994: National Strategic Intelligence Act: Section 2[1] (b)
- [6] Act 92 of 1982: Nuclear Energy Act, Section 68
- [7] Act 102 of 1980: National Key Points Act, Section 10
- [8] Act 4 of 2013: Protection of Personal Information (POPI) Act
- [9] 32-138: Vetting Administration Procedure.

2.2.2 Informative

- [10] MISS: Minimum Information Security Standards [1996].

2.3 Definitions

Classification	All official matters, including documents, photographs, plans, sketches, drawings, voice and video recordings, computer based presentations, schedules, agendas, minutes of meetings requiring the application of security measures, i.e. exempted from disclosure, shall be classified “ Confidential ”, “ Secret ” or “ Top Secret ”
Top Secret	the classification given to information that may be used by malicious/ opposing/ hostile elements to neutralise the objectives and functions of an organisation
Secret	the classification given to information that may be used by malicious / opposing / hostile elements to disrupt the objectives and functions of Eskom Holdings SOC Limited
Confidential	the classification given to information that may be used by malicious / opposing / hostile elements to harm the objectives and functions of Eskom Holdings SOC Limited

Controlled Disclosure	the manner in which a document or information is disclosed with appropriate consent and to authorised persons
Classified Information	sensitive information which is in Eskom’s interest, is held by, is produced in or is under the control of Eskom, or which concerns Eskom and which shall, because of its sensitive nature, be exempted from disclosure and has to be protected against being compromised
Classified Item	an item that forms part of or contains classified information
Copying/ duplicating/	making a copy of any document, whether copying it out by hand,

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

reproducing	reproducing it by photographic or any other means
Document	<p><i>In terms of the Protection of Information (Act 84 of 1982) a document is:</i></p> <ul style="list-style-type: none"> 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
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
Security screening/ vetting	the systematic process of investigation followed in determining a person's security competence
Communication Security	that condition created by the conscious provision and application of security measures for the protection of classified communication
Eskom	Eskom Holdings SOC Limited, its divisions and any other business entities in which Eskom has a controlling interest, either by its capital interest and/ or voting rights.
Register	a register kept by the Head of Department in which all such documents is recorded
HOD	Head of Department who are authorised to handle or who stores it
Author	the author of a the classified items generated
Line Manager	the direct/ responsible manager of an employee
Control Register	The register containing all classified items handled by an appropriate office

2.4 Abbreviations

Abbreviation	Explanation
GCE	Group Chief Executive (Eskom Holdings SOC Ltd)
BU	Business Unit
SOC Ltd	State Owned Company Limited
SSA	State Security Agency
HOD	Head of Department in Eskom
NDI	Non-Disclosure of Information
NDA	Non-Disclosure Agreement

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

2.5 Roles and Responsibilities

2.5.1 The HOD must

- a) Determine in his/ her department all job-positions where incumbents may be exposed to classified information;
- b) Determine the classification of such information (as per 3.2);
- c) Inform the incumbent of such determination;
- d) Ensure that all incumbents are vetted to the required level in terms of the Vetting Administration Procedure;
- e) Ensure that all incumbents are informed and comply with this procedure; and
- f) Keep a control register.

2.5.2 The Originator of the document must

- a) Apply for a security clearance on the prescribed SSA form, obtainable from Security Division, and
- b) Comply with the prescripts of this document.
- c) What is the role of Security Division and SBI???

2.6 Process for Monitoring

As prescribed within the organisational quality management system pertaining the handling and storage of records and documentation.

2.7 Related/Supporting Documents

Not applicable

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

3. Procedure for Handling Classified Items

3.1 Reason for classification

Items are classified in an attempt to ensure that the efficient functioning of Eskom 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 SSA.

3.2 Non-Disclosure of Information

No person, employed by Eskom on a permanent or on a 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 DE Security.

3.3 Classification of items

3.3.1 Levels of classified item

- a) **Top Secret:** This classification will be allocated only to technical, intellectual, commercial or financial information of an extremely sensitive nature, where disclosure will lead to irreparable harm to Eskom. This type of information must be circulated with extreme prejudice. Items may only be classified as "Top Secret" by a person possessing a security clearance at this level.
- b) **Secret:** This classification will be allocated only to information that has the potential to harm the technical, intellectual, commercial or financial interests of Eskom, or one of Eskom's contractors. Items may only be classified as "Secret" by a person possessing a security clearance at this or a higher level.
- c) **Confidential:** This classification will be allocated only to information that is potentially harmful or embarrassing to Eskom. This allocation may only be authorised by a person who has a security clearance at this, or a higher level.
- d) **Controlled Disclosure:** This form of classification only refers to the disclosure of a documentation, information or items to other employees or persons.

3.3.2 General Rules regarding Classified Items

- a) *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.*
- b) The classification of an item will be determined by the highest grade of that the classified item contains. The same classification as that of the original shall be assigned to any extracts from that document.
- c) 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.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- d) 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. When the State Security Agency (Domestic Branch) declares that an employee cannot be cleared for whatever reason, and it is essential that he/ she has access to classified items, the supervising managers have to proceed with great caution in order to prevent any breaches of security. Such person will be required to sign a "Declaration of Secrecy"

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 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 under lock and key and be periodically collected by an officer designated to do this, and destroyed by burning or shredding. Computer generated draft material shall be stored in secured and or encrypted media.
- c) The author of a classified document shall indicate thereon whether it may be reclassified after a certain period or upon the occurrence of a particular event. This option has to be applied consistently in the case of documents with a classification of "Confidential" or higher.
- d) Where the recipient of a classified document is of the opinion that such document should be reclassified, he/ she have to 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 and will remain in the original format.
- f) Only typists who have the necessary clearance may type classified 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.
- g) Classified files should be opened only when an actual need arises, not merely because the filing system provides for the existence of such a file.
- 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.
- i) A register shall be kept of all classified files opened/in existence. As and when a file is opened, the particulars have to be entered in the register. The register itself will be classified to at least "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.
- 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 taken out of the room where such files are kept (which **should not** be common practice), an entry has to be made on the sub-file indicating to whom and when the main file has been issued.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- l) No file is allowed to remain outside the dedicated room for longer than one working day. Classified files shall be enclosed in a lockable folder or container at all times when 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.

3.5 Marking 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.

3.6 Distribution

Classified information may only be disclosed to persons who “**NEED TO KNOW**” and the number of such persons shall be restricted to the minimum.

3.6.1 Copies

- a) Where possible, extracts rather than copies should be made of classified items.
- b) Copies 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 normally have access to those items.
- c) No copies of **Top Secret** and **Secret** items shall be allowed.

3.6.2 Internal circulation

- a) All Secret/ Top Secret classified items to be circulated internally (within the same locality) shall be taken to the addressee personally by a specifically designated person who, in turn, has to be in possession of a security clearance and may not be circulated by internal mail.
- 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 three (3) copies of internal

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

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 dispatched 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.

3.6.3 External circulation

a) Receipt and distribution of documents

- The responsible manager shall appoint a person to be responsible for the receipt 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
- Any item classified **Top Secret** or **Secret**, which is dispatched, made available or distributed, shall be registered in order to ensure control
- When **Top Secret** or **Secret** documents are dispatched, made available or distributed, the addressee is required to give a written acknowledgement of receipt. Such acknowledgement of received documents will, in turn, be kept in a secure location.

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 (*currier by hand, registered post, facsimile or computer*), registered number of postal material, signature of the recipient (*currier, registration person dispatching*), receipt number and date when receipt was obtained.
- 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 information item in a new envelope, seal it and address it. Then stamp the security classification on the front and sign across the flaps of the envelope. Envelopes marked Confidential in the printing process may also be used.
- The seams of the inside envelope shall be properly sealed by paper seals, counter-signed 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".

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- 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 in the appropriate manner. A receipt to be signed by the recipient and returned to the sender has to 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 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 should be equipped with a combination lock.
- Couriers shall have at least a "*Confidential*" security clearance and, wherever possible, be accompanied by a second person.
- The courier has to 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 has to be exercised over the time taken by a courier to deliver the documents. Upon receipt, the recipient has to check that the items have not been compromised.
- Couriers have to 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.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- 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.
- b) Classified (Secret /Top Secret) items may not be taken home unless proper lock-up facilities exist there, and such removal of classified items has to be approved in writing by the head of the department or his/her dually 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/ electronically with password
 - **“Secret”**: Strong room or reinforced lockable filing cabinet within a security controlled area. Electronic documentation should be stored and encrypted with 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 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 security locks. The keys to a room, safe-deposit or cabinet in which classified items are stored have to be properly tended and effective key control shall be exercised. Duplicate keys and the codes of combination locks shall be kept in a sealed envelope by the departmental head and combination codes should be changed at regular intervals.
- c) The combinations of the locks of a strong room or safe shall be changed every three months and also 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 when the code had necessarily been disclosed to another person.

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- No unauthorised person may be present when the new combination is set or the lock is opened.
- d) Proper access control and control over movement inside any building or part of a building in which classified items are handled has to 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 security locks 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 metal cabinet of adequate strength that is 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 not working there. 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. Persons who have to gain access to such building after hours should be duly authorised by the head of the department or his/her delegate.
- h) No classified item may be stored offsite or outside the control of Eskom, unless authorised by the author/ HOD/ Line manager or summonsed 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 standard concerning the retention period for documents;
- b) Where destruction has been properly 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 has destroyed the items shall give the head of the department a certificate of the destruction of 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 has to make provision for the destruction, storage and/ or moving of classified items in the event of an emergency, in order to prevent the risk of items being compromised. The possibility of off-site storage with a reputable firm must be reported to security to be investigated.
- f) The destruction of classified items in electronic or soft copy format need to comply by the standards and procedures set by the Group IT Division.

3.10 Loss of classified items

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

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

- b) 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.
- c) If a breach of security occurs or when classified documents become lost, the general manager/ BU manager concerned will request a confidential investigation.
- d) If necessary, a board of inquiry consisting of a representative from the organisation segment where the document was lost, a representative from 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) Declassification: When a security classification becomes obsolete due to changed circumstances, only the author of the document shall declassify the document to a lower level of classification and notify all the persons concerned.
- b) Reclassification: When 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 the 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 that classified items.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
J Mogaswa	Middle Manager: Security Division
K Pillay	Middle Manager: Security Division
A Govender	Middle Manager: Security Division
R Rajpal	Middle Manager: Security Division
R Moodley	Middle Manager: Security Division
F Diergaardt	Middle Manager: Security Division
M Heath	Middle Manager: Security Division
J Cheerkoot	Middle Manager: Security Division
M de Jenga	Middle Manager: Security Division
M Murugen	Middle Manager: Security Division

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.

5. Revisions

Date	Rev.	Compiler	Remarks
December 2003	0	PJ Fouche	Added Reference ESKADABT3
February 2008	0.1	PJ Fouche	Revised + converted to a procedure + unique ID 32-143
October 2010	1	PJ Fouche	Reviewed and reformatted procedure
April 2014	2	A Govender	Reviewed procedure
March 2016	3	LP Human	Reviewed procedure
September 2016	4	P Malitsha	Reviewed procedure
September 2016	4.1	R Dreyer	Reviewed procedure
November 2016	4.2	R Dreyer	Update and format of procedure

6. Development Team

This document originated from an integrated team within the Security Division and was revised by the Security Business Intelligence Department

7. Acknowledgements

Not applicable

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Ltd, Reg No 2002/015527/30.