

	STANDARD	Group Information Technology
---	-----------------	-------------------------------------

Title: **INFORMATION SECURITY
LOGICAL ACCESS CONTROL**

Document Identifier: **32-351**

Alternative Reference :
Number

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

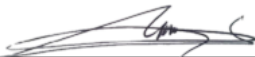
Functional Area: **Information Security**

Revision: **6**

Total Pages: **16**

Next Review Date: **April 2027**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
		
R Netshishivhe Chief Advisor – IT Security Services	S Gama Middle Manager – Cyber Security	S Songo Senior Manager – IT Security Services
Date: 02 / 04 / 2024	Date: 02/04/2024	Date: 04-04-2024

Content

Page

1. Introduction	4
2. Supporting Clauses.....	4
2.1 Scope	4
2.1.1 Purpose	4
2.1.2 Applicability	5
2.2 Normative/Informative References.....	5
2.2.1 Normative	5
2.2.2 Informative.....	5
2.3 Definitions.....	6
2.3.1 Classification	6
2.3.2 Other	6
2.4 Abbreviations.....	6
2.5 Roles and Responsibilities.....	7
2.6 Process for Monitoring.....	8
2.7 Related/Supporting Documents	8
3. Standard	8
3.1 Request Logical Access	8
3.1.1 General	8
3.1.2 Supporting Documentation	9
3.2 Granting Logical Access	10
3.2.1 User Identification and Authentication.....	10
3.3 Resetting and GENERATING Passwords.....	11
3.3.1 Resetting Passwords.....	11
3.3.2 Generating Passwords	12
3.4 Monitoring and Reviewing Logical Access	12
3.4.1 Monitoring Areas	12
3.4.2 Recertification.....	12
3.4.3 Deviations.....	12
3.5 Maintaining user Access.....	12
3.5.1 Dormant Accounts	12
3.5.2 Updating User Information.....	13
3.5.3 Removing Logical Access.....	13
3.6 Encryption	13
3.7 Security Controls	14
3.7.1 Automatic Lockout	14
3.7.2 Automatic Time-outs.....	14
3.7.3 Access to Classified Information.....	14
3.7.4 Privileged access.....	15
4. Acceptance	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.

5. Revisions 16

6. Development Team..... 16

7. Acknowledgements..... 16

1. Introduction

Logical access to an organisation's information resources needs to be managed in a controlled manner and logical access permissions should be granted on the basis of business requirements. Lack of adequate logical access controls could lead to unauthorised access to systems, information and information resources.

Eskom management has recognised this threat and has therefore formulated this **32-351 Information Security – Logical Access Control Standard** in order to address the related risks.

2. Supporting Clauses

2.1 Scope

This standard is applicable to logical access to information systems and technology, owned and managed by Eskom, and any personal computers and/or servers authorised to access Eskom's technology networks. The scope of this standard also extends to computing equipment within the plant process-computing environment.

This standard applies to, but is not limited to, the following:

- Applications;
- Databases;
- Operating systems;
- Source code;
- Workstations i.e. PCs;
- Networks;
- Interfaces;
- Mobile devices i.e. cell phones

Specific procedures and guidelines to facilitate the implementation of this standard shall be established within Divisions and business units.

2.1.1 Purpose

The purpose of this standard is to ensure that logical access to information resources is controlled and managed based on business requirements.

Eskom aims to protect information resources, as classified per *32-369 Information Security – Physical Asset Classification and Control Standard* and *32-438 Information Security – System Classification Standard*; and effectively manage risks in the environments in which it operates. This standard shall ensure the implementation of appropriate logical access control measures so as to manage the risk of:

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.

- Breach of confidentiality;
- Breach of integrity;
- Lack of system availability;
- Reputational damage; and
- Financial loss through the loss of confidential Eskom information.

2.1.2 Applicability

This standard applies to Eskom Holdings Limited, its divisions and subsidiaries and their employees, including temporary staff, contractors, consultants, third parties and service providers making use of Eskom's information technology resources.

2.2 Normative/Informative References

The following documents contain provisions that, through reference in the text, constitute requirements of this standard. At the time of publication, the versions referenced were valid. All controlled documents are subject to revision, and parties to agreements based on this standard are encouraged to reference the most recent versions of the listed documents. Information on currently valid national and international standards and specifications can be obtained from the Information Centre and Eskom Documentation Centre at Megawatt Park.

2.2.1 Normative

- [1] 32-85: Information Security Policy
- [2] 32-435: Information Security – End User Usage and Computing Standard
- [3] 32-359: Information Security – Access Control Procedure.

2.2.2 Informative

- [1] ISO27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements
- [2] ISO 9001 Quality Management Systems
- [3] 32-370: Information Security – Systems Development Standard.
- [4] 32-376: Information Security – Third Party Access Standard.
- [5] 32-373: Information Security – Remote Access Standard.
- [6] 32-362: Information Security – Incident Management Procedure

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.

2.3 Definitions

2.3.1 Classification

- a. **Public domain:** published in any public forum without constraints.
- b. **Controlled disclosure:** controlled disclosure to external parties.
- c. **Confidential:** the classification given to information systems and technology that may be used to **harm** the objectives and functions of Eskom Holdings Limited.
- d. **Secret:** the classification given to information systems and technology that may be used to **disrupt** the objectives and functions of Eskom Holdings Limited.
- e. **Top Secret:** the classification given to information systems and technology that may be used to **neutralize** the objectives and functions of Eskom Holdings Limited.

2.3.2 Other

- a. **Audit Trail:** A record, or series of records, that allows the identification of activities on an application, database, and network device.
- b. **Source code:** The code written/created by the developer/programmer before compilation thereof into an application.
- c. **Information systems:** Any computer application or database, as well as a combination thereof, that assists in the processing and/storage of information and data;
- d. **Information technology:** Any hardware device, e.g. computer, network switch, router, etc. that facilitates the use, or access to, an information system;
- e. **Logical Access:** Ability of users, applications or devices to obtain the use of features or functions of an information system or technology.
- f. **Users:** Any person who has been granted logical access to an information system or technology.
- g. **Forms:** This could be an electronic or paper-based document that must be completed with information;
- h. **Eskom:** This refers to Eskom Holdings SOC Limited, its divisions and wholly owned subsidiaries.
- i. **Third party:** Persons/organisations that are not part of an Eskom Division and/or Eskom's subsidiary companies, connecting to the Eskom network from a location outside Eskom's control.

2.4 Abbreviations

Abbreviation	Description
CIO	Chief Information Officer
EDC	Eskom Documentation Centre
EIAM	Enterprise Identity Access Management

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.

Abbreviation	Description
ID	Identification
IT	Information Technology
PC	Personal Computer

2.5 Roles and Responsibilities

ROLE	FUNCTIONAL RESPONSIBILITIES
Eskom Information Security Manager	- Review and update Eskom Information Security Standard in order to mitigate identified risks to the organisation. - Communicate to all stakeholders the content and changes made to Eskom Information Security Standards. - Ensure compliance of this Eskom Information Security Standard and report non-compliance issues to stakeholders and Eskom service providers, where relevant.
Information Manager	- Assist with the implementation of standards and procedures with input from all Stakeholders. - Identify and evaluate Information Security risks according to the Eskom Integrated Risk Management Methodology and request counter measures from the Information Security department to address these risks. - Ensure compliance of this standard within the division and report non-compliance issues.
IT Service Provider	- Implement and comply with the Information Security Standards and procedures for Eskom. - Continuously monitor and report to the relevant SLA manager - Provide Information Security trend reports as required and propose solutions to address these possible risks.
Line Manager	Approves logical access requests in accordance with this standard.
System Administrators	Implement and comply with the Logical Access Standard in the management and maintenance of the systems assigned to their custody.
User	Comply with the requirements of the logical access standard.

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.

2.6 Process for Monitoring

The efficacy and applicability of this Standard will be monitored continuously to ensure continuous compliance thereto, and relevance thereof to Eskom. The following measures must be taken:

- a. Generate a recurring report that identifies the following accounts:
 - Password has not changed in more than 30 days;
 - Dormant accounts, i.e., accounts that have not been accessed for more than 30 days. The inactivity should be restricted to 30 days in the case of service accounts and accounts with elevated privileges.
- b. Generate a recurring report showing granted, changed, revoked and / or suspended access rights and the reasons and signoffs by relevant management. The reasons can include but are not limited to:
 - Users that leave Eskom employment;
 - Suspension of users on leave;
 - Suspension of users disciplined;
 - Suspension and/or revocation of inactive users (based on monitoring of access);
 - Termination of contracts.
 - Privileged users and their access rights

2.7 Related/Supporting Documents

- eForm - User network registration
- eForm - Application form system access
- eForm - Remote access

3. Standard

3.1 Request Logical Access

3.1.1 General

- a. The authorised Access Request forms shall be completed whenever access to any information resources within Eskom is requested (*32-359 Information Security – Access Control Procedure*).
- b. The Access Request form shall collect the following at a minimum.
 - Name and Surname of requestor;
 - User ID;
 - Telephone number;

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.

- Physical location;
 - Cell phone number (required if user wish to receive an SMS for password reset);
 - Cost centre;
 - Line Manager's name;
 - System/Application;
 - Business reason for access;
 - Authorisation from the Line Manager;
 - Period access required / Revocation date.
- c. The access request shall be approved by the following parties to authorise the requested access:
- User's line manager – to ensure that the requested access is indeed needed and that all other details supplied are correct; e.g. business reason submitted with the form.
 - Applicable information or system owner.
- d. The final approved access request form shall be routed to the logical access administrators or the relevant system administrator to provision the user.
- e. A central registry must be maintained of all access requests.

3.1.2 Supporting Documentation

- a. A system authorisation list shall be created and kept up to date. This list shall, as a minimum, contain the following information:
- Name of the system;
 - Persons who may authorise access to the system;
 - Level of access rights for which the person may authorise access.
- b. Each information or system owner shall create and maintain an access control matrix, ensuring that proper segregation of duties is established, in order to simplify the granting of logical access to systems. The matrix shall include the following:
- Type of work performed;
 - Systems needed for the work performed;
 - Classification of information that is needed to perform work;
 - Type of access that must be granted in order for the user to perform the work;
 - Segregation of duties requirements; and
 - Duration the access may be granted for.

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.

3.2 Granting Logical Access

Logical access shall be granted in accordance with the applicable governance rules as per this Standard. The principle of “Least privilege” shall be adhered to when granting access. The following lists the basic verification points:

- Access shall only be granted upon successful completion of the authorised access request process.
- Access shall only be granted with the authorisation of the relevant information or system owner.
- Only the approved access rights, as per the access request application, shall be granted.

3.2.1 User Identification and Authentication

- a. All users shall be issued with a uniquely identifiable User ID.
- b. Prior to being granted access to information resources, all users shall have their identity verified with their User ID and password.

3.2.1.1 User ID Management

- a. All logical access administrators shall consistently observe the user ID naming standards, except where an application for an exception has been made.
- b. The use of a shared user ID for a group of users or a specific task shall not be allowed.
- c. No duplicate user IDs shall be allowed.
- d. The User ID shall be suspended the moment the employee is suspended, employment terminated or contract has expired.
- e. Users shall not be allowed to have multiple log-on sessions on the same system, unless appropriately authorised by the Information or System owner.
- f. Anonymous and/or guest user IDs shall be disabled on all systems, except where the system explicitly requires the anonymous and/or guest ID to effectively perform its expected function.
- g. Every User ID created for a non-permanent employee shall have an expiration date specified, with a default expiration of 30 days where the actual expiration is unknown.
- h. Error or information messages at login shall convey the minimum information required so as not to divulge the full reason for an unsuccessful login.

3.2.1.2 User Responsibility

- a. Users shall be held responsible for all activities performed with their User IDs.
- b. Users shall not share User IDs and passwords.
- c. The user shall only access systems for which he/she has been authorised to access.
- d. The user shall not use hacking and/or probing programs designed to gain unauthorised access or compromise user accounts, to any system or application.
- e. The user shall ensure the safe storage of passwords, tokens and other devices used for access
- f. The user shall not include clear-text passwords in an automated log-on process.

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.

- g. Whenever there is an indication of possible password compromise, the user shall change the password or Report the incident through the Incident Management Procedure (32-362 *Information Security – Incident Management Procedure*).

3.2.1.3 Password requirements

- a. User passwords shall be a minimum of eight (8) characters long and consist of a combination of letters (Uppercase and lowercase) and numbers. Special characters shall be used where possible.
- b. Password strength verification shall be performed by the various systems, that the user has access to, when logging onto the specific system. Strength verification on password shall test that the password is adhering to the minimum length, as defined for the specific system or application and is not weak, e.g. 123456 as password.
- c. Users' passwords shall be set to expire every thirty (30) days. Passwords of accounts with privileged access, e.g. administrator, root; service accounts, etc. shall expire every 20 days. If there are any exceptions to this and system passwords cannot be changed often, a formal exceptions process must be followed.
- d. As a minimum the previous five (5) passwords shall be recorded to prevent re-utilisation. Where possible, twelve (12) previous passwords shall be recorded.
- e. Passwords shall at all times be entered in non-display fields.
- f. Passwords shall be encrypted when transmitted over any network and when in storage.

3.2.1.4 Guidelines on Creating a Good Quality Password

- a. String several words together also known as a password phrase, e.g. At the red car - @theredcar.
- b. Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word, e.g. school – s2h4o6
- c. Combine punctuation or numbers with a regular word, e.g. 2cool4school.
- d. Deliberately misspell a word but do not use a common misspelling, e.g. Durbanbeach1 – Durb@nb3ach1.

3.3 Resetting and GENERATING Passwords

3.3.1 Resetting Passwords

- a. Users are required to use the Self-Service Password Reset functionality offered by Eskom to reset their passwords. If this functionality is not available then the user may call the Eskom Helpdesk for assistance;
- b. The Eskom Helpdesk will issue the user with a temporary password and guide the user to use the Self-Service Password Reset functionality;
- c. The identity of a user, who requires a password reset, will be verified.
- d. If a user cannot be positively identified then the password shall not be reset and the user shall have to provide physical identification and written consent of password reset from his/her manager.

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.

3.3.2 Generating Passwords

- a. The logical access administrators shall generate temporary passwords in line with the guidelines on creating a good quality password for users as discussed in paragraph 3.2.1.4: Guidelines for creating a Good Quality Password.

3.4 Monitoring and Reviewing Logical Access

3.4.1 Monitoring Areas

- a. The following areas shall be monitored depending on criticality as decided:
 - Authorised access;
 - Date and time of logical access events;
 - Unauthorised logical access attempts;
 - Failed logical access attempts;
 - Logical access Standard violations;
 - The actual access rights and the authorised access rights;
- b. Logical access rights shall be amended as, and when, required.

3.4.2 Recertification

Recertification is the process of verifying and confirming the access rights granted to users. This process is required to ensure that active users still need the access granted and prevent rights accumulation.

- a. Line Managers shall review the access rights granted to the members of their team on a quarterly basis, or when there have been changes in the team and their resultant access rights.
- b. Privileged users shall have their access rights reviewed on a monthly basis by the System Owner

3.4.3 Deviations

- a. The logical access administrators shall ensure that all access rights are in line with business needs. Any deviations shall be investigated and reported to the Division Information Manager.
- b. All unauthorised access rights shall be revoked with immediate effect.

3.5 Maintaining user Access

3.5.1 Dormant Accounts

Accounts not used for an extended period of time demonstrate that no access to information on that system is needed. The continued existence of these accounts on production systems pose a risk to Eskom insofar as it can be used to perpetrate fraud or other unauthorised activities.

- a. Recurring reports shall be generated to identify accounts that had been inactive (dormant) for 30 days.

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. These reports shall be sent to the relevant Line Managers, or Information Manager, to determine the status of the user of each dormant account.
- c. If the user's employment had been terminated, or the access is no longer required, then the relevant account must be suspended and de-provisioned from all production systems.
- d. If the user will require the account at a later stage then the account must be suspended on all provisioned applications – the Line / Information Manager must provide a reason for the continued requirement of the account in a production system.
- e. Recurring reports shall be generated to track the action taken with regard to identified dormant accounts.

3.5.2 Updating User Information

- a. Human Resources as well as the Information Owner shall inform the Information Manager of organisational changes, e.g. structural changes, appointments, moves and resignations impacting access lists.

3.5.3 Removing Logical Access

User and service accounts created in a user directory will not be deleted but disabled and maintained in a separate container to provide historical information to Eskom when required.

Please refer to the document, *Information Security – Access Control Procedure*, for more details regarding the removal of logical access.

- a. User accounts shall be de-provisioned from all systems to which the user had been granted access when the following conditions occur:
 - The user's employment contract with Eskom is terminated;
 - The user's employment/contract with an Eskom business partner is terminated;
 - The relationship between Eskom and the business partner, for whom the user works, is terminated;
 - An external party, e.g. customer is found to have abused his/her logical access to Eskom systems;
 - The CIO has issued an instruction, with a business reason, to remove access from an account.
- b. Logical access rights that are no longer required, as identified in paragraph 3.4.2 Recertification, shall be removed as soon as these have been identified.
- c. User IDs shall not be re-used and the list of previously used UIDs must be referenced by the IAM system when generating new UIDs. This serves to minimise the risk of access rights being inherited by a new user.

3.6 Encryption

- a. Encryption shall be implemented as per the 32-387 Information Security Encryption Standard.
- b. Encryption of passwords shall be applicable for all passwords being stored or transmitted.

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.

3.7 Security Controls

3.7.1 Automatic Lockout

- a. User accounts must be locked after three (3) unsuccessful login attempts.
- b. Service accounts and other privileged accounts must be locked after three (3) unsuccessful login attempts.

3.7.2 Automatic Time-outs

- a. Inactive system sessions, i.e. where no activity had been detected, shall be protected through the activation of a password-protected screen saver. The screen saver shall be activated after five (5) minutes of inactivity.
- b. Where possible, inactive system sessions shall be automatically terminated after ten (10) minutes.
- c. Users shall not attempt to circumvent automatic time-out controls, by implementing measures such as pinging the server to maintain connection.

3.7.3 Access to Classified Information

For information about access to information that has been classified, refer to 32-438 Information Security – System Classification Standard.

3.7.3.1 Public Domain / Non-Classified and Controlled Disclosure

- a. The minimum password requirements as set out in this document shall be in place to authenticate access to information classified as Controlled Disclosure in the Eskom environment, e.g. Eskom Intranet.
- b. Public Domain / Non-classified information do not require passwords.

3.7.3.2 Confidential

- a. The minimum password requirements as set out in this document shall be in place to authenticate access to information classified as Confidential.
- b. Multi-factor authentication shall be used to gain access to confidential information. Authentication shall be based on a password and a One-Time PIN.

3.7.3.3 Secret

- a. The minimum authentication requirements as set out in this document shall be in place to access information classified as Secret.
- b. Multi-factor authentication shall be used to gain access to confidential information. Authentication shall be based on a password and a One-Time PIN.

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.

3.7.4 Privileged access

3.7.4.1 Additional Identification

- a. The number of privileged user IDs shall be strictly limited to those individuals who require such privileges for authorised business purposes (*32-359 Information Security – Access Control Procedure*). A risk assessment shall be performed by Eskom Information Security to identify any risks that may be inherent to the users' logical access profile before approval of privileged access rights.
- b. The direct use of privileged accounts such as Root, System and Administrator is not allowed. Authorised users should be issued with an account with the relevant elevated privileges to fulfil their administrative duties.
- c. Privileged user IDs shall not be used to perform normal day-to-day work.
- d. The use of privileged user IDs shall be recorded and logged.
- e. A list of the privileged user IDs and encrypted passwords shall be stored in a secure location for Disaster Recovery purposes (*32-372 Information Security – Physical and Environmental Standard*). These IDs shall be tested on a monthly basis to ensure that they are applicable (*32-358 Information Security – IT Continuity Management Standard*).

3.7.4.2 Additional Authentication

The minimum authentication requirements shall be in place for privileged accounts.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Faith Burn	Chief Information Officer
Sithembile Songo	Senior Manager – IT Security Services
Anthenia Phuku	Senior Manager – Business Solutions and Development Services
Varsha Pillay	Senior Manager – Applications Operations
Tebogo Makhwelo	Senior Manager – Infrastructure Operations
Norbit Williams	Senior Manager – IT Governance Services
Ian Marks	Senior Manager – Specialised Technical Services (Acting)

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
January 2008	0	K.M. Sekgaphane	A standard with document number EST 32-351 was developed and published on the Eskom Documentation System.
January 2010	1	M.O.K. Motshoane	EST 32-351 was revised and published.
June 2012	2	N.M. Rapuleng	EST 32-351 was revised and published
July 2014	3	T. Mayayise	EST 32-351 was revised
October 2018	4	R. Netshishivhe	EST 32-351 was revised and published
March 2023	5	R. Netshishivhe	EST 32-351 was revised and published
March 2024	6	R. Netshishivhe	EST 32-351 was revised and published

6. Development Team

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

- Information Security Team

7. Acknowledgements

N/A

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.