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

Title: **Information Security Systems
Classification Standard**

Document Identifier: **32-438**

Alternative Reference
Number: **N/A**

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

Functional Area: **Group IT**


Revision: **4**

Total Pages: **15**

Next Review Date: **October 2020**

Disclosure Classification: **Controlled Disclosure**

Compiled by



M Thipe
**Acting Information
Security Manager**

Date: 30/10/2018

Functional
Responsibility



T Makhwelo
**Senior Manager ITSO
Technical Services &
Governance**

Date: 30/10/2018

Authorized by



N Zibi
**Acting Chief Information
Officer**

Date: 01/11/2018

Content

	Page
1. Introduction.....	3
2. Supporting Clauses	3
2.1 Scope.....	3
2.2 Purpose.....	3
2.3 Applicability	3
2.4 Effective date	3
2.5 Normative/Informative References	3
2.6 Normative.....	4
2.7 Definitions	5
2.7.1 Classification	5
2.7.2 Other	5
2.8 Abbreviations	6
2.9 Roles and Responsibilities	6
2.10 Process for Monitoring.....	7
2.11 The system owner must have a BIA report/output not older than 24 Months. Related/Supporting Documents	7
3. Standard.....	7
3.1 Ownership	7
3.2 The Information Classification System.....	7
3.3 System Owner.....	8
3.4 Classification Levels.....	8
3.4.1 Confidentiality.....	8
3.4.2 Integrity	9
3.4.3 Availability	9
3.5 Classification of systems	10
3.5.2 Factors to consider when determining classification Levels of systems	10
3.6 Reviewing and Maintaining Classification	11
3.6.1 Confidentiality controls	11
3.6.2 Integrity controls	13
3.6.3 Availability controls	14
4. Acceptance.....	15
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

Multifactor authentication is an IT security technology technique that involves users to provide numerous forms of identification or information to authorize the validity of their identity for an online transaction or in order to be granted access to corporate applications. The foremost goal of the multifactor authentication methods is to upsurge the difficulty with which an attacker can exploit the login process to freely wander around the corporate networks and compromise Information System's resources to take and steal confidential information of the organization.

2. Supporting Clauses

2.1 Scope

This standard covers all systems residing on data networks, servers, mainframes and personal computers (stand-alone or network-enabled) located at Eskom and non-Eskom locations, where these systems are under the jurisdiction and/or ownership of Eskom, and any personal computers and/or servers authorised to access Eskom's data networks..

2.2 Purpose

The purpose of this document is to ensure that systems receive an appropriate level of protection in accordance with their importance to the organization and to establish standard controls to be implemented for the different classification levels of systems within Eskom.

2.3 Applicability

This standard applies to Eskom Holdings Limited, its divisions and subsidiaries, including temporary staff, contractors, service providers and consultants utilising Eskom's information resources.

2.4 Effective date

From the day of approval

2.5 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 editions indicated were valid. Controlled documents are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of the documents listed below. Information on currently valid national and international standards and specifications can be obtained from the Information Centre and Eskom Documentation Centre at Megawatt Park.

- [1] 32-85 Information Security Policy
- [2] 32-86 Eskom Integrated Risk Management Policy

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] 32-351 Information Security – Logical Access Control Standard
- [4] 32-372 Information Security – Physical and Environmental Security Standard
- [5] 32-361 Information Security – Change Control Procedure

2.6 Normative

- [1] ISO 27001 Information technology — Security techniques — Information security management systems — requirements
- [2] ISO 9001 Quality Management Systems Informative

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.

2.7 Definitions

2.7.1 Classification

- a. **Public domain:** published in any public forum without constraints (either enforced by law, or discretionary).
- b. **Controlled disclosure:** controlled disclosure to external parties (either enforced by law, or discretionary).
- c. **Confidential:** the classification given to information that may be used by malicious/opposing/hostile elements to **harm** the objectives and functions of Eskom Holdings Limited.
- d. **Secret:** the classification given to information that may be used by malicious/opposing/hostile elements to **disrupt** the objectives and functions of Eskom Holdings Limited.
- e. **Top Secret:** the classification given to information that may be used by malicious/opposing/hostile elements to **neutralize** the objectives and functions of Eskom Holdings Limited.

2.7.2 Other

- a. **Availability:** The property of being accessible and usable upon demand by an authorized entity
- b. **Backup:** The process whereby copies of information or systems are taken in order to allow recreation of the original, should the need arise.
- c. **Eskom:** is used for Eskom Holdings Limited, its divisions and subsidiaries.
- d. **Integrity:** The property of safeguarding the accuracy and completeness of information assets
- e. **System:** Is a combination of computer components working together i.e. an application system or operating system. An application system is an IT implementation of a business system or process.
- f. **System Classification:** The process of assigning ratings to a system, based on its confidentiality, integrity and availability requirements, in order to determine the level of protection that needs to be afforded to the system.
- g. **System Owner:** A user responsible for assigning a system, classification and alerting Group IT to implement appropriate safeguards and controls to protect the system and the data as per the classification scheme.

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.

2.8 Abbreviations

Abbreviation	Explanation
CE	Chief Executive
ED	Executive Director
EDC	Executive Document Centre
GIT	Group IT
IT	Information Technology

2.9 Roles and Responsibilities

Roles	Responsibilities
Information Security Manager	<ul style="list-style-type: none">➤ Review and update Eskom Information Security Standards in order to meet Eskom 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.➤ Evaluate potential risks to Eskom and introduce counter measures to address these risks based on System Classification.➤ Co-ordinate the implementation of new or additional security controls for systems based on their classification.
Information Manager	<ul style="list-style-type: none">➤ 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 Policy 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	<ul style="list-style-type: none">➤ Implement and comply with the Information Security Standards and procedures for Eskom➤ Continuously monitor and report to the Information Security Manager.➤ Provide Information Security trend reports in Eskom and propose solutions to address these possible risks
Information Owner	<ul style="list-style-type: none">➤ The Information Owner shall be responsible for determining the classification of systems under their control.➤ The Information Owner shall review, and maintain, all classified systems on a regular basis.
System Owner	<ul style="list-style-type: none">➤ The system owner shall enforce the security controls as per the defined classification of the information processed by the system.
Computer User	<ul style="list-style-type: none">➤ Shall comply with all information security policies, standards and procedures for System Classification.

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.

2.10 Process for Monitoring

The following reports shall be drawn and reviewed to assess compliance with this standard:

- The system owner must produce an annual show a verification of control/demonstration of controls as required by the classification standard.

2.11 The system owner must have a BIA report/output not older than 24 Months. Related/Supporting Documents

3. Standard

3.1 Ownership

All systems implemented and maintained for Eskom operational and business purposes are the property of Eskom, unless:

- Eskom has contractually agreed otherwise; or
- The system is the property of another party by operation of law.
- All users accessing Eskom systems shall have the responsibility to preserve the confidentiality, integrity and availability of the information residing within these systems.
- All Eskom systems shall have a designated system owner. Whenever there is no system owner it must assigned to the business process owner or IM,
- The Owners of information systems shall be accountable for their classification.
- Classifications and associated protective controls for systems shall take account of business needs for sharing or restricting information, as well as legal requirements.

3.2 The Information Classification System

The system classification system shall be:

- Simple;
- Usable;
- Acceptable;
- Supported by automated means;
- Meaningful, e.g. classifications expressed in business terms;
- Applicable to all types of systems in use within Eskom;
- Scalable;
- Easy to apply to both new and legacy systems;
- Easy to maintain;
- Enforceable;

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.

- Capable of being applied consistently;

The minimum-security controls as specified for all the categories of the system classification shall be applied to all systems classified in each category.

The controls that will be in place include the following:

- Access to classified systems;
- Handling of information of classified systems;
- Labelling of information;
- Integrity checks;
- Recovery and availability.

3.3 System Owner

- The System Owner shall be the person who has been allocated responsibility for a system and who is accountable in the event of loss or destruction of the system or parts thereof.
- If the system does not have a clearly defined System Owner, then the Information Manager shall be deemed to be the System Owner.
- The System Owner shall bear responsibility for ensuring that the system has been appropriately classified and that control measures applied to the system are in line with its classification.

3.4 Classification Levels

3.4.1 Confidentiality

The following classification levels shall be applied when assessing the confidentiality of a system:

- **Public Domain / Non-Classified**

Definition: Published in any public forum without constraints (Either enforced by law or discretionary)

- **Controlled Disclosure**

Definition: Controlled disclosure to any external parties (Either enforced by law or discretionary)

- **Confidential**

Definition: the classification given to information that may be used by malicious/opposing/hostile elements to **harm** the objectives and functions of Eskom Holdings Limited.

- **Secret**

Definition: the classification given to information that may be used by malicious/opposing/hostile elements to **disrupt** the objectives and functions of Eskom Holdings Limited.

- **Top Secret**

Definition: the classification given to information that may be used by malicious/opposing/hostile elements to **neutralise** the objectives and functions of Eskom Holdings Limited.

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.

Confidentiality ratings may also be applied to stand-alone pieces of information which exists outside of systems.

When assessing the confidentiality of the system, consider the following questions:

- How can a malicious party (internal or external) use the system to cause harm to Eskom?
- Would loss of confidentiality of the system violate laws, regulations, contractual obligations or Eskom policies?

3.4.2 Integrity

The following classification levels shall be applied when assessing the integrity of the system:

- **Low**

Definition: the loss of integrity of information will have a low adverse impact on Eskom i.e. Eskom will be able to continue primary functions, minor financial losses may result and some confusion may be experienced.

- **Moderate**

Definition: the loss of integrity of information will have serious impact on Eskom i.e. Eskom will be able to continue primary functions but effectiveness is significantly reduced, significant financial loss is experienced, public confidence may be reduced, management decisions are adversely influenced

- **High**

Definition: the loss of integrity of information will have catastrophic impact on Eskom i.e. primary functions cannot continue, major financial loss is experienced, public confidence may be destroyed, major reputational damage is caused, public confidence is severely reduced.

3.4.3 Availability

The following classification levels shall be applied when assessing the availability of the system:

- **Low**

Definition: the loss of availability of information will have a low adverse impact on Eskom i.e. Eskom will be able to continue with primary functions, minor financial losses may result, minor damages to Eskom's assets may occur.

- **Moderate**

Definition: the loss of availability of information will have serious impact on Eskom i.e. Eskom will be able to continue primary functions but effectiveness is significantly reduced, significant financial loss is experienced, significant damage to Eskom's assets may occur

- **High**

Definition: the loss of availability of information will have catastrophic impact on Eskom i.e. primary functions cannot continue, major financial loss is experienced, major damage to Eskom's assets may occur.

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.

3.5 Classification of systems

- a. System classifications shall be recorded as a combination of the confidentiality, integrity and availability classifications using the format System Name (Confidentiality rating, integrity rating, availability rating) e.g. SAP (Confidential, Moderate, High)
- b. Where a single system is used for a variety of purposes and could potentially have varying degrees of classification, the highest classification afforded to any individual component of the systems shall be considered as the overall system classification
- c. Where a system consists of various components, but a decision has been taken to classify the system cumulatively, the highest classification afforded to any individual component of the systems shall be considered as the overall system classification.
- d. All information that resides in systems will take the default classification of the system unless classified otherwise by the Information Owner.
- e. If uncertainty arises relating to the classification level that needs to be assigned, the higher rating shall be assigned.
- f. Where a system classification has not been assigned, a default classification of (Controlled disclosure and Moderate) shall be assumed.
- g. Whilst the Information owner bears responsibility for agreeing the overall classification of a system, various stakeholders may be involved in making decision regarding system classifications.

3.5.2 Factors to consider when determining classification Levels of systems

- In assessing the confidentiality, integrity and availability levels of a system, relevant legislation, regulations, contractual clauses and the value of a system shall be considered.
- The value of a system is not used to determine the classification of the system, but the value of the information assets processed by the system will be important in determining cost effectiveness of implementing the appropriate safeguards to the system.
- When assessing the integrity classification of a system, consider the impact that unauthorised modification or deletion of the system (or parts thereof) may have in terms of the following:
 - Reducing public confidence
 - Creating potential for fraudulent financial gain
 - Creating confusion or controversy through false attribution of incorrect information
 - Influencing personnel and management decisions
 - Interfering with law enforcement or legal processes

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.

3.6 Reviewing and Maintaining Classification

- The Information Owner shall assign, review and maintain classification of systems under their control
- The Information Owner shall ensure that adequate protection is in place to protect the system in line with its classification.

The following information shall be added to the document registry whenever the classification of systems is reviewed:

- The date the review took place;
- Persons involved in the review;
- Changes to the classification of the information.

When downgrading classification levels:

- Assess the risks related to the loss of confidentiality, integrity and availability prior to downgrading the classification according to the 32-86 Eskom Integrated Risk Management Policy;
- Destroy or declassify surplus classified materials.

3.6.1 Confidentiality controls

The table below defines the minimum security controls that need to be in place for systems, depending on the confidentiality classification of the system. For each confidentiality classification level, the controls to be applied shall include those defined for the prior level together with new controls defined for the assigned level:

System confidentiality classification	Minimum controls required
Public Domain / Non-Classified	None
Controlled Disclosure	Controls shall be in place to prevent external access to this system. (Refer to the 32-351 Eskom <i>Information Security – Logical Access Control Standard</i> and 32-85 <i>Information Security Policy – End-user and Computing</i>). These shall include the following: <ul style="list-style-type: none">• Authorised access to the Eskom network
Confidential	Controls shall be in place to prevent external access to this system. (Refer to the 32-351 Eskom <i>Information Security - Logical Access Control Standard</i>). These shall include the following: <ul style="list-style-type: none">• User identification and authentication (username and password);• Logging use at level of individual; Technological controls as per the approved Eskom standards and applicable processes

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.

System confidentiality classification	Minimum controls required
	<p>(i.e. firewalls, IPS, etc)</p> <ul style="list-style-type: none"> Building security shall be utilised to prevent physical access to the system or information manually stored outside of the system (refer also to the 32-372 Eskom <i>Information Security – Physical and Environmental Security Standard</i>). When information is transmitted outside the system, it shall be encrypted as per the 32-387 Information Security Encryption Standard and accompanied by a notice stating that it is internal to Eskom and may not be disclosed to anyone who is not an Eskom employee. Notification or destruction instructions shall be included in the notice to instruct anyone who incorrectly receives the information. Copies of information from the system shall only be made for internal use. Information within the system shall be disposed of by deleting or overwriting the information as per the 32-372 Information Security – Physical and Environmental Security Standard
Secret	<ul style="list-style-type: none"> Access shall be limited to authorised personnel only. Dual authentication mechanisms (strong authentication) shall be applied. Access to the system shall at all times be logged. Server room security controls shall be utilised to prevent physical access to the hardware housing the system. Access to the server room shall be restricted to authorised personnel only. All access to the server room shall be logged and monitored. (Refer also to the Eskom <i>Information Security – 32-372 Physical and Environmental Security Standard</i>). Information within the system shall be encrypted during storage and transmission, using Eskom-approved encryption mechanisms as per the 32-387 Information Security Encryption Standard. Copies of information from the system may only be made upon approval by the system owner. The destruction of information from the system shall be witnessed and shall be recorded in the Document Registry. Information from the system residing on electronic media shall be disposed by degaussing or overwriting the information or physically destroying the media as per the 32-372 Information Security – Physical and Environmental Security Standard
Top Secret	<ul style="list-style-type: none"> Access shall be strictly restricted to the minimum number of authorised personnel, on a need-to-know basis. Electronic Top Secret information shall be protected against unauthorised internal use or intrusion by external parties through multi factor authentication, potentially including biometric authentication.

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.

System confidentiality classification	Minimum controls required
	<p>Intrusion detection shall be applied at all times.</p> <p>Top Secret information shall only be copied from systems or removed from Eskom premises:</p> <ul style="list-style-type: none">• If the information is needed for a declared purpose;• If the person removing the information has written authorisation from the system owner and the divisional head.

3.6.2 Integrity controls

The table below defines the minimum security controls that need to be in place for systems, depending of the integrity classification of the system:

System integrity classification	Minimum controls required
Low	<ul style="list-style-type: none">• Periodic checks shall be performed by the system owner to ensure that the system integrity is maintained.
Moderate	<ul style="list-style-type: none">• Periodic checks shall include the use of reconciliations or independent verification.• The system code shall be verified prior to implementation.• All information moving in and out of the system shall be verified for integrity before use.• An independent source may be used to verify the integrity of information.• Core functionality/transactions within the system shall be segregated.• Physical access to the system shall be limited to authorised personnel (refer also to the 32-372 <i>Eskom Information Security – Physical and Environmental Security Standard</i>)
High	<ul style="list-style-type: none">• Automated measures shall be implemented to verify the integrity of information transmitted to/from the system (e.g. use of hash totals and checksums).• Access to the system shall be strictly controlled.• Segregation of duties shall be enforced on the system and these shall be reviewed every 6 months by the system owner.• Additional measures shall be implemented to safeguard physical access to the system and limit access to a minimum number of personnel.

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.

3.6.3 Availability controls

3.6.3.1 Safety & Revenue Critical Tier 0

Failure of system function may result in injury or death to human beings and/or significant loss of revenue.

- **Time loss/RTO**
 <8 hours
- **Data Loss/RPO**
 = 0

3.6.3.2 Mission Critical Tier 1

Vital to the functioning of an organization and the accomplishment of its mission.

- **Data Loss/RPO**
 <24h
- **Data Loss/RPO**
- **=0**

3.6.3.3 Business Critical Tier 2

Without which the business can still continue operations for a pre-defined time period.

- **Time loss/RTO**
 <48 hours
- **Time loss/RPO**
 <24 hours

3.6.3.4 Business Essential Tier 3

Without which the system can still continue operations for after 5 days.

- **Time loss/RTO**
 <5 days
- **Data Loss RPO**
 <24 hours

3.6.3.5 Normal Tier 4

Without which the business can still continue operations for up to a month.

- **Time loss/RTO**
 >5 days
- **Time loss/RPO**

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 days

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Nondumiso Zibi	Acting CIO and Group Executive
Bhavesh Reddy	Acting Senior Manager – Business Solutions
Nomsa Vanda	Acting Senior Manager – Analytics Centre of Excellence
Grasswell Mabudusha	Senior Manager – IM Business Relationship Management
Ian Marks	Acting Senior Manager – Office of the Chief Information Officer
Maureen Mokone	Senior Manager – Business Process Management & SEA
Nico Harris	Senior Manager – IM Operations
Varsha Pillay	Acting Senior Manager – ITSO Shared Services
Sham Dhrampal	Corporate Specialist (SSE) – Enterprise Architecture
Tebogo Makhwelo	Senior Manager – ITSO Technical Service and Governance
Neo Lemao	Senior Advisor IT Compliance

5. Revisions

Date	Rev.	Compiler	Remarks
January 2008	0	K.M. Sekgaphane	A Standard with document number EST 32-438 was developed.
September 2008	1	M.O.K. Motshoane	Content of EST 32-438 was revised, in alignment with South African Regulatory requirements.
January 2010	2	M.O.K. Motshoane	EST 32-438 was revised and published.
June 2012	3	N Hlela	EST 32-438 was revised and published.
December 2017	4	M Phofu	Document updated

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.