Eskom	**Policy**	

Title: **Acceptable Use of Information and Information Systems Policy**

Document Identifier:	**240-103449776**
Alternative Reference Number:	
Area of Applicability:	**Eskom Holdings SOC Ltd**
Functional Area:	**Group IT – ITSO TSG**
Revision:	**2**
Total Pages:	**14**
Next Review Date:	**November 2024**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Functional Responsibility**	**Authorised by**
		Burn
M Singo	**S Songo**	**F Burn**
Chief Advisor – IT Security Services	**Senior Manager – IT Security Services**	**Chief Information Officer**
Date: 10/12/2021	Date:10-12-2021	Date: 10 December 2021

Contents

1. Introduction

Eskom Holdings SOC Ltd (Eskom), as a state-owned company (SOC), possesses information that is sensitive and valuable and is, therefore, obliged to ensure that such information is protected against unauthorised use or disclosure. The exposure of sensitive information to unauthorised individuals or its use brings the organisation's brand into disrepute, resulting in harm to the organisation. This could also result in Eskom being subjected to fines or other legal sanctions.

This policy provides management direction regarding the acceptable use of information and information systems. It provides principles for acceptable practices of Eskom's information and information systems as outlined in the ISO 27001/27002 security standards.

This policy applies to all Eskom employees, contractors, third parties, and/or agents.

While Eskom permits acceptable personal use, for example, electronic banking, of its information systems, employees should be aware that these are subject to the terms and conditions contained in this policy, the conditions of employment, as well as any contracts signed between Eskom and third-party vendors.

Information security is seen as the preservation of confidentiality, integrity, and availability of information.

2. Policy content

2.1 Policy statement

The acceptable use of information and information systems in Eskom is critical to the success of the organisation, and it must be protected against misuse.

2.2 Policy principles or rules

2.2.1 Employment

2.2.1.1 Acceptable usage before employment/engagement

a. Employees must read all policies relating to the acceptable use of information and information systems and sign the non-disclosure agreements related to such.

b. Access to systems and information by Eskom employees and also by third parties must be granted based on the least privilege principle, "need to know", and approved work authorisation.

c. Eskom Holdings' employees and third parties must take cognisance that information and information systems and services provided by Eskom are the property of Eskom and must be used for the purpose of facilitating and supporting Eskom business.

2.2.2 Acceptable usage during employment/engagement

2.2.2.1 Acceptable usage: general use

Users shall report all information security incidents promptly.

2.2.2.2 Acceptable usage: Eskom devices

a. All users shall use their own unique user ID and password to access Eskom's information resources.

b. Users should take suitable precautions to guard Eskom's devices against the environmental threats of fire, theft, flood, hazardous material, and excessive ambient temperature/humidity.

2.2.2.3 Acceptable usage: working off-site/remote working

a. Users shall only access Eskom's network and information resources for business purposes and acceptable personal use.

b. Users shall not bypass approved methods of accessing IT systems.

c. Users shall not probe or in any manner assist any other person in probing security mechanisms at either Eskom or other non-Eskom Internet sites, unless authorised.

d. Users shall ensure that suitable security controls are implemented on their mobile device in order to protect Eskom's information resources.

e. Users must not leave their mobile devices unattended or active while connecting to Eskom information or information systems remotely.

f. Users shall take reasonable control measures to secure their Eskom devices when traveling.

g. Users shall ensure that the location for remote working is safe and secure.

h. It is the user's responsibility to report a lost Eskom device within a reasonable period not exceeding two working days.

2.2.2.4 Acceptable usage: Internet

a. Users shall not use the Internet inappropriately, as they may be subjected to disciplinary action, which, in serious cases, may result in dismissal. Refer to the definition of acceptable and/or unacceptable use and related categories.

2.2.2.5 Acceptable usage: email

a. Eskom employees shall not use their personal email address to conduct Eskom's business; only an Eskom email address must be used.

b. Eskom contractors who require the use of their own business email address to conduct Eskom business must obtain approval from Eskom.

c. Users are not allowed to address or respond to any Eskom client or colleagues regarding Eskom business-related matters using their private email accounts. This must be from the Eskom email service.

d. Users are prohibited from the following activities:

    1. Creating, storing, forwarding, printing, or distributing chain letters or offensive material
    2. Sending, forwarding, and/or distributing any Eskom information to any unauthorised users, individuals, or parties without prior approval
    3. Sending non-business-related email messages to email distribution groups and/or to all Eskom personnel without prior approval

4. Sending, forwarding, and/or distributing any email messages that can bring Eskom into disrepute or can damage the Eskom brand
5. Attempting to impersonate (logging on using another user's username, password, or token) other Eskom users by sending non-work and/or work-related material
6. Using active animated programs or graphics of any nature in email signatures or as background to email messages

2.2.2.6 Acceptable usage: printing

a. To minimise printing costs, users shall utilise the printing services for business purposes when it is necessary to do so.
b. Users shall employ secure printing using a pin code at all times.
c. Users shall retrieve printed documents from the printer immediately after the print job has gone through.

2.2.2.7 Acceptable usage: mobile computing

a. All personal mobile computing devices used to access Eskom-managed data shall be passcode-enabled.

b. All personal mobile computing devices used to access Eskom-managed data should be running the latest version of the operating system available, and all the latest patches should be applied.

c. Antimalware software with the latest signature files shall be active at all times on all personal computers.

2.2.2.8 Acceptable usage: handling of classified information

a. Users shall not forward, disclose, and/or make copies of Eskom's information to external parties without the explicit permission of the information owner.

2.2.2.9 Acceptable usage: storage and backup

a. Users are responsible for managing, backing up, and storing their work-related documents on Eskom's approved document management platforms.

2.2.2.10 Acceptable usage: digital and social media

a. Users shall not engage in social-media-related activities that may bring Eskom into disrepute.
b. Users shall not use social media to attack Eskom or its stakeholders.
c. Users are required to conduct themselves in a manner aligned with Eskom values as and when they utilise social media services.
d. Users shall not post confidential information about Eskom or its stakeholders without the specific authorisation to do so.
e. Users shall not post nor comment on work-related matters through social media, unless authorised to do so.
f. Users are not permitted to visit sites or create, transmit, or download material that contravenes local law or presents documents about race and sexual content, pornography, terrorist activities, and obscene or defamatory content.

2.2.3 Acceptable usage on termination of employment/engagement

a. All employees/third parties must return all Eskom information, information-processing devices, and assets before leaving Eskom's service.

b. All data, assets, or intellectual property developed or gained during the period of employment or service at Eskom remains the property of Eskom and must not be retained beyond the termination of service, be divulged to anyone, or reused for any purposes. Confidentiality of Eskom's information must be maintained after leaving Eskom's service.

c. Eskom employees whose employment has been terminated are prohibited from the following activities:

   i. Intentionally disposing of Eskom information, maliciously affecting Eskom information systems, or interrupting Eskom operations

   ii. Copying, duplicating, and removing any Eskom information for use outside the organisation

2.3 Interception

Eskom is permitted to intercept communications in accordance with the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act. Any interception of communications shall be strictly in accordance with the requirements of this Act as well as in accordance with the requirements of the Protection of Personal Information (POPI) Act, as and when required.

2.4 Consequences of unacceptable use

Eskom reserves the right to revoke access to an Eskom device/asset and/or suspend or terminate access to the service on notice of abuse, violation, or attempted violation of this policy. Furthermore, it is a violation of this policy to use the services of another company for the purpose of facilitating any of the activities set out in the preceding section if such use of another company's service could reasonably be expected to affect the service in any manner.

Violation of this policy will be treated as a breach, and the disciplinary process will be followed.

If any provision of this policy is rendered invalid under law, such provision shall be deemed modified or omitted to the extent necessary, and the remainder of this policy shall continue in full force and effect.

No purported relaxation or waiver of this policy shall be valid, unless reduced to writing and signed by Eskom's Executive Committee or its delegates, alternatively, as sanctioned by a valid Eskom policy and/or standard to this effect. Unless specifically indicated to the contrary, any such relaxation or waiver shall relate only to the specific request received and employee concerned and shall not be of general application.

Accordingly, in response to any given violation, Eskom may impose penalties ranging from the termination of the user's access to the information and information systems, to disciplinary action or further action, including, but not limited to, non-reappointment, discharge, or dismissal in accordance with the Eskom Disciplinary Code, Procedure, and Directives. In cases involving serious violations, Eskom may institute legal action or co-operate with an action brought by applicable authorities or third parties. All exceptions to this policy shall be formally recorded, tracked, and reviewed by the Information Security Unit and communicated to the relevant users.

2.5 Suspected information security breach or incident

It is the user/employee's responsibility to report all suspicious activities or suspected breaches of information security policies and standards without delay to both the line manager and Information Security Department. These breaches or incidents may also be reported to the Information Security team for investigation purposes by emailing infosecurity@eskom.co.za. All (potential) breaches will be investigated. Where investigations reveal misconduct, disciplinary action will follow in line with the Eskom disciplinary procedures.

2.6 Policy Compliance

- Compliance Measurement

The IT Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and/or external audits, and feedback to the policy owner.

- Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3. Supporting clauses

3.1 Scope

This policy is mandatory for all Eskom employees and/or divisions that handle Eskom information and information systems.

All divisions must fully meet the provisions as outlined in this policy.

This policy contains principles and rules for information security that are applicable to all Eskom divisions.

3.1.1 Purpose

The purpose of this policy is to provide management direction and guidance regarding the acceptable use of Eskom's information and information systems. It provides principles for acceptable practices with regard to Eskom's information and information systems.

3.1.2 Applicability

This policy applies to:

a. all divisions within Eskom Holdings SOC Ltd and its subsidiaries;

b. all employees, temporary employees, contractors, subcontractors, vendors, third parties, service providers, and business partners of Eskom, that is, all users of Eskom's information, information systems, and information resources, regardless of their status (contract, permanent, or otherwise), collectively referred to in this policy as users or end users; and

c. all subsidiaries and other consolidated entities, including consolidated joint venture (JV) entities, and consistently from these entities down the subsidiary JV ownership chain.

The above are collectively referred to in this document as “divisions”, “employees”, and/or “third parties”.

3.1.3 **Effective date**

This policy is effective from the date of approval.

3.2 Normative/Informative references

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

3.2.1 Normative

[1] 32-527: Ethics Policy

[2] 32-86: Risk Management Policy

[3] 32-727: SHEQ Policy

[4] 32-85: Information Security Policy

[5] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

[6] Protection of Personal Information Act 4 of 2013

[7] 32-1112: Eskom Disciplinary Code

[8] 32-1113: Eskom Disciplinary Procedure

[9] Cybercrimes Act 19 of 2020

3.2.2 Informative

[10] ISO CobiT DS5 Process/CobiT 4.1

[11] British Standard 25777 Information and Communication Technology Continuity Management Code of Practice

[12] Interception and Monitoring Prohibition Act 127 of 1999

[13] Electronic Communications and Transactions Act 25 of 2002

[14] National Archives and Records Service Act 43 of 1996

[15] Harassment Act 17 of 2011

[16] ISO 9001 Quality Management Systems – Requirements

[17] ISO 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements

[18] ITIL Information Technology Information Library 3.0

[19] Minimum Information Security Standards

3.3 Definitions

Term	**Definition**
Abuse	Improper usage or treatment of an entity, that is, computer system/services, often to unfairly or improperly gain benefit.
Excessive	More than is necessary, normal, or desirable use of computer systems and/or services for non-business activities.
Portable/Mobile devices	Reference to, but not limited to, devices such as laptops, notebooks, slates, mobile devices, iPads, and tablets.
Information assets	Computers, laptops, iPads, desktops, printers, photocopiers, and any device that has the capability of storing, processing, and retrieving information.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Information system	An integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, and digital products. This includes, but is not limited to, Eskom devices, servers, networks, and services, as well as information assets.
Classified information	Information that has been classified into any of the following categories: **top secret**, **secret**, **confidential**, and **controlled disclosure**.
Top secret information	The classification given to information that may be used by malicious, opposing, or hostile elements to neutralise the objectives and functions of Eskom Holdings Limited.
Secret information	The classification given to information that may be used by malicious, opposing, or hostile elements to disrupt the objectives and functions of Eskom Holdings Limited.
Confidential information	The classification given to information that may be used by malicious, opposing, or hostile elements to harm the objectives and functions of Eskom Holdings Limited.
Controlled disclosure	Controlled disclosure to external parties (either enforced by law or discretionary).
Social media platform	Social media are interactive technologies that allow the creation or sharing/exchange of information, ideas, interests, and other forms of expression via virtual communities and networks. Examples of social media are Twitter, WhatsApp, YouTube, Facebook, Instagram, Telegram, etc.
Public	Published in any public forum without constraints (either enforced by law or discretionary).

Term	**Definition**
Acceptable personal use	Usage that does not consume more than a trivial amount of resources, it does not interfere with the user’s productivity, and it is not used for charitable or private business activities.
Unacceptable personal use	Usage that consumes a trivial amount of resources and/or interferes with the user’s productivity, and/or usage for charitable or private business activities, and/or brings Eskom into disrepute.
Unacceptable Internet categories	Internet categories that are not acceptable on Eskom information resources. Examples of unacceptable Internet categories include, but are not limited to: • child pornography; • dynamic DNS host; • gore/extreme; • hacking; • malicious outbound data/botnets; • malicious sources/malnets; • pornography; • potentially unwanted software; and • proxy avoidance. Streaming, social media, and television are also not recommendable, as they might negatively affect the network bandwidth, unless these are used for business purposes.

3.4 Abbreviations

Abbreviation	Explanation
ID	Identification
IT	Information technology
ITSO	Information Technology Service Operations
POPI	Protection of Personal Information Act 4 of 2013

3.5 Roles and responsibilities

The chief executive, executives, and managers are responsible for the implementation of this policy.

Role	Responsibilities
Divisional executives	• Divisional executives shall ensure that the necessary acceptable usage practices are implemented and complied with as per this policy.
Information Security	• Co-ordinate the overall communication and awareness strategy for information security. • Establish and co-ordinate appropriate working group forums to facilitate organisation-wide representation and feedback on information security. • Co-ordinate the implementation of new or additional information security controls.
Information manager	• Ensure that all computer users are aware of the applicable policies, standards, procedures, and guidelines for information security. • Review the effectiveness of Eskom's information security strategy and implemented information security controls. • Ensure compliance with this policy within the group, and report deviations to the Information Security middle manager.
Managers	• Ensure that employees read, understand, and agree to abide by the controls set in this policy. • Ensure that individuals are given clear direction to the extent and limitations of their authority with regard to information and information systems. • Provide written authorisation for the use of the information systems and devices. • Ensure that, on termination of service, the user's access is removed from all Eskom systems. • Ensure and confirm that all Eskom and non-Eskom employees (contractors, auditors, third parties, etc.) have deleted all Eskom information from their non-Eskom devices on termination of service. • Investigate all reports of the loss of Eskom mobile devices, and implement remedial action, including, but not limited to, disciplinary action, where deemed appropriate.
Computer user	• Comply with all acceptable usage policies, guidelines, and procedures for information security. • Be aware of all updates made to acceptable usage policies, guidelines, and procedures for information security.

Role	Responsibilities
	• Classify and handle data/information in accordance with Eskom's Information Classification Standard (32-438). • Immediately report any suspicious, suspected, and actual security incidents, weaknesses, compromises, and breaches to the relevant security body in Eskom. • Report a lost Eskom mobile device within a reasonable period not exceeding two working days.
Corporate Legal Department	• Investigate special incidents that involve misconduct, unethical behaviour, and any other form of incident as and when requested by the Information Security middle manager.
Human resources management	• Ensure that all employees are fully aware of the existence and contents of this policy and their legal responsibilities with respect to their use of the information and information systems. Such responsibilities are to be included in the employee documentation such as the terms and conditions of employment. • Ensure that all new employees undergo all necessary (security) screening before employment and gaining access to Eskom's information and information systems.

3.6 Process for monitoring

Compliance with the Acceptable Use of Information and Information Systems Policy will be monitored through the following methods:

a. Annual user surveys to verify that the policies are both applied and understood
b. Physical inspection (that is, walkabout for spot checks on the clear desk policy)
c. Conformance reviews
d. The regular review of this policy
e. Compliance audits regarding this policy
f. Regular audits by the Assurance teams to ascertain compliance with this policy

Specific control requirements incorporated in this policy may be applied to a third party. In such cases, obtaining the agreement of the third party to the control requirement(s) and the monitoring of, and oversight over, the effective operation of the related controls will be the responsibility of the relevant accountable sector head.

3.6.1 Management process

The policy mandates minimum levels of information security controls that must be practised by all Eskom divisions, including employees, third parties, and contractors accessing Eskom's information and information systems. Divisions must provide evidence of compliance with these expectations, where necessary or required. The Information Security Department will ensure group-wide awareness of this acceptable use policy and obtain support and understanding in terms of accountability for, and compliance with, this policy.

Group IT and information security incidents can be logged through this email address: itcare@eskom.co.za or telephone number: 0860 724 365.

3.6.2 Implementation

The policy will be implemented in the following fashion:

The Information Security Department will formulate and communicate group-wide awareness surrounding this policy.

Divisional heads, as well as line managers, are accountable for ensuring adherence to, and implementation of, this policy within their respective areas.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Faith Burn	Chief Information Officer
Mmabatho Singo	Senior Manager – IT Security Services (Acting)
Tebogo Makhwelo	Senior Manager – Infrastructure Operations
Ian Marks	Senior Manager – Specialised Technical Services (Acting)
Anthenia Phuku	Senior Manager – IM Business Solutions and Development Services
Varsha Pillay	Senior Manager – Applications Operations
Leocardia Kamanga	Senior Manager – IT Governance Services
Grasswell Mabudusha	Senior Manager – Strategic Project Services

5. Revisions

Date	Rev.	Remarks
January 2016	0.1	New policy document (Draft 1)
November 2018	1	New policy document
November 2021	2	Reviewed document

6. Development team

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

- Mmabatho Singo – Chief Advisor Information Security
- Ronald Netshishivhe – Chief Advisor Information Security
- Mabongi Ngidi – Senior Advisor Information Security
- Neo Lemao – Senior Advisor Information Security

7. Acknowledgements

Not applicable.