Eskom	Directive	

Title: **Vetting and screening of Security Service Providers**

Document Identifier: **559-27048273**

Alternative Reference Number:	**Not applicable**
Area of Applicability:	**Eskom Holdings SOC Ltd**
Functional Area:	**Group Investigations and Security**
Revision:	**1**
Total Pages:	**10**
Next Review Date:	**January 2028**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
Romeo J Malgas	Botse Sikhwitshi	Tembela Kulu
Middle Manager Vetting	Senior Manager SBI	General Manager Investigations and Security
Date: 03-02-2025	Date: 03 February 2025	Date: 25/02/2025

Content

1. Introduction

In line with the Minimum Information Security Standard (MISS) and the National Strategic Intelligence Act, 1994 (Act No 39 of 1994) and as Amended through the General Intelligence Laws Amendment Act 11 of 2013 Eskom as a state-owned entity is obliged to comply with these laws in place to ensure protection of critical infrastructure and information kept or produced.

2. Directive Content

2.1 Directive Statement

Eskom as a state-owned entity shall ensure that all prospective security service providers are vetted by the relevant authority (State Security Agency & Eskom Vetting Fieldwork Unit) before being deployed to any of Eskom's areas, including but not limited to all its Divisions and Subsidiaries. This vetting process must be completed before any security personnel are deployed to Eskom's areas.

2.2 Directive Principles or Rules

Security vetting and screening as a counter-intelligence measure is essential to these protective principles integral to the organisation:

- Deny access to unauthorised persons.
- Safeguard information from foreseeable risks.
- Promote individual accountability for the protection of information, processes and systems and ensure that disclosures and access to information are managed according to the need-to-know principle.
- Ensure that effect is given to the legal provisions and use of non-disclosure and declarations of secrecy agreements in contractual, partnering or employment relationships.
- Promote the integrity, control, and security competence of people, processes, and systems.
- Facilitate the preservation and appropriate sharing/dissemination of official and business information within the required protocols and rules of the business.
- Comply with the statutory, contractual, and business requirements for security vetting.

3. Supporting Clauses

3.1 Scope

This Directive is applicable to all prospective security service providers throughout Eskom, its Divisions and Subsidiaries, appointed directly by Eskom, a Division or Subsidiary. This Directive is also applicable to Divisions or Subsidiaries where security services might be sourced on a subcontracting basis e.g., NTCSA Project Delivery and Eskom Rotek Industries. This includes all security services and security technology installations covered by the Private Security Industry Regulating Authority (Psira) Act and South African Intruder Detection Services Association (SAIDSA).

3.1.1 Purpose

The aim of this directive is to protect Eskom, its people and assets by ensuring all security service providers are vetted by the relevant authorities (State Security Agency & Eskom Vetting Fieldwork Unit) before any agreements/contracts are placed and or entered between the parties concerned.

3.1.2 Applicability

This Directive applies throughout Eskom Holdings SOC Limited, its divisions, wholly owned subsidiaries and entities within South Africa wherein Eskom have a controlling interest, operating in terms of South African law.

3.1.3 Effective date

This Directive is effective when published.

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] 32-138: Vetting Procedure.

[2] Minimum Information Security Standards (MISS) [1996].

[3] National Strategic Intelligence Act, 1994 (Act No 39 of 1994).

[4] General Intelligence Laws Amendment Act 11 of 2013.

[5] Risk and Integrity Management Framework (RIMF) for State Owned Companies [2020].

[6] 240-145382935: Declaration of Secrecy – MISS Annexure B.

[7] Minimum Physical Security Standards (MPSS) [2015].

[8] 32-85: Information Security Policy.

[9] 240-55410927: Cyber Security Standard for Operational Technology.

[10] 240-53716911: Overarching Group IT Policy.

[11] Private Security Industry Regulation Act 56 of 2001 as amended.

[12] National Key Point Act 102 of 1980.

[13] Critical Infrastructure Protection Act 8 of 2019.

[14] Nuclear Energy Act 46 of 1999.

[15] Interception and Monitoring Prohibition Act of 1995.

[16] Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002.

[17] Electronic Communications and Transactions Act 25 of 2002.

[18] Electronic Communication Act 68 of 2002.

[19] Prevention of Organised Crime Act 121 of 1998.

[20] Protected Disclosures Act 26 of 2000.

[21] Protection of Information Act 84 of 1982.

[22] Protection of Personal Information Act 24 of 2013.

[23] Promotion of Access to Information Act 2 of 2000.

[24] 32-1112: Disciplinary Code Standard.

[25] 32-1113: Disciplinary Procedure for Bargaining Unit Employees.

3.2.2 Informative

[1] ISO 28000 Specifications for Security Management Systems.

[2] King III & IV report on Corporate Governance.

[3] Companies Act 71 of 2008.

[4] National Vetting Strategy of South Africa, 2006.

[5] 32-86: Integrated Risk Management Policy.

[6] 32-727: Safety, Health, Environment and Quality Policy.

[7] 32-527: Eskom Code of Ethics Policy.

[8] 32-757: Code of Ethics Procedure.

[9] 32-1186: Private Work Policy.

[10] Public Finance Management Act 1 of 1999.

[11] Eskom Contract Management Framework

[12] National Treasury Regulations

[13] B-BBEE Codes of Good Practice of 2013

[14] Eskom's Integrity Pact with Suppliers

3.3 Definitions

Definition	Explanation
Security Vetting	Is the prescribed and systematic process of investigation (vetting investigation) followed in determining a person's security competence. Security vetting can be done pre- or post-employment.

Screening	This entails verifying the identity, qualifications, civil or criminal liability records, previous work history, financial soundness, professional registrations, and integrity, status, and records of individuals and/or vendor/contractors including those held by the South African Police Service (SAPS) Criminal Record Centre (CRC) but not limited thereto.
Security Competence	A person's ability to act in such a manner that he/she does not cause classified information or material to fall into unauthorised hands, thereby harming or endangering the security or interests of the state. Security competence is normally measured against the following criteria: susceptibility to extortion or blackmail, amenability to bribes, susceptibility to being compromised due to inappropriate behaviour, and loyalty to the state/institution.
Security Clearance	An official document/certificate indicating the degree of security competence of a person issued to a candidate after a security vetting investigation. It indicates the degree of a person's security competence and specifies the level of classified information to which the candidate may have access, subject to the need-to-know principle. A security clearance is a key for granting access to classified information and for determining the person's integrity, but is not a guarantee, and does not confer any rights. It is intended to counter the following threats: espionage, corruption and related crimes, organised crime syndicates; and an exodus of skills and secrets.
Vetting Authority	The State Security Agency (SSA) which is established by the Constitution and regulated by the National Strategic Intelligence Act (NSIA) that is consistent with the Constitution. SSA conducts vetting investigations as a counterintelligence mechanism to protect national security.
Vetting Field Unit (VFU)	As defined in paragraph 2A (5A) of the General Intelligence Laws Amendment Act (Act 11 of 2013) and established by means of a memorandum of understanding between State Security Agency and a Government Department, Organ of State- or State-Owned Entity, to conduct vetting investigations on behalf of the SSA.
Classified Information	Sensitive information which, in the national interest, is held by, is produced in, or is under the control of the State, or which concerns the State, and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise. Such information is classified as Confidential, Secret or Top Secret.
Confidential	The classification is limited to information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of an individual and/or institution.

Secret	The classification is given to information that may be used by malicious/opposing/hostile elements to disrupt the objectives and functions of an institution and/or state.
Top Secret	The classification is given to information that can be used by malicious/opposing/hostile elements to neutralise the objectives and functions of institutions and/or state.
Security	The use of security measures in the physical and logical domains is designed to deny unauthorised access to information, facilities, equipment, systems, processes, computers, networks, and resources, and to protect individuals and property from damage or harm. It involves the use of multiple layers of interdependent systems, processes, and techniques for protection purposes.
Security Manager	A person appointed to manage all matters relating to the administration and organisation of security at the site/department/business unit and division.
Need-to-Know Principle	The furnishing of only that classified information or part thereof that will enable a person(s) to carry out his/her/their task.
Declaration of secrecy	An undertaking given by a person who will have, has, or has had access to classified information, that he/she will treat such information as secret (MISS Appendix B, a draft declaration that can be modified to suit the requirements in each case).
Counterintelligence	This means measures and activities conducted, instituted or taken to impede and neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct vetting investigations and to counter any threat or potential threat to national security.
Compromise	The unauthorised disclosure/exposure or loss of sensitive or classified information, or the exposure of sensitive operations, people, or places, whether by design or through negligence.
Document	In terms of the Protection of Information Act (Act 84 of 1982) means: • 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 another device in or on which sound or any signal has been recorded for reproduction.
Document Protection	The deliberate provision and application of security measures to protect classified information.

Eskom Subsidiaries	Eskom Holdings SOC Ltd is the main operating company. The Eskom group comprises the operating company and its wholly owned subsidiaries.
Procurement and Supply Chain Management	Procurement and supply chain management is the business management function that ensures identification, sourcing, access and management of the external resources that an organisation needs or may need to fulfil its strategic objectives. Procurement and supply management involves buying or leasing or disposing the goods and services that enable an organisation to operate in a profitable and ethical manner.

3.4 Abbreviations

Abbreviation	Explanation
CIPA	Critical Infrastructure Protection Act 8 of 2019
MISS	Minimum Information Security Standard
MoU	Memorandum of Understanding
NKP	National Key Point
Psira	Private Security Industry Regulating Authority
P&SCM	Procurement and Supply Chain Management
SAIDSA	South African Intruder Detection Services Association
SSA	State Security Agency
SVIS	Security Vetting Information System
VFU	Vetting Fieldwork Unit

3.5 Roles and Responsibilities

3.5.1 Group Security Vetting Fieldwork Unit (VFU)

The VFU must ensure all request for vetting or screening by the relevant Division or Subsidiary are quality checked, captured on the SVIS system and submitted to the State Security Agency on a weekly basis, in line with the SSA submissions accepting process. The VFU must further use the available tools and systems to extract all information relevant to the screening of the service provider and submit report/s as part of the official drafted request to the State Security Agency for final screening assessment and feedback.

The VFU is responsible to request and obtain status feedback from the State Security Agency. The VFU will submit the feedback report from the SSA to the relevant P&SCM practitioner as soon as such is received from the State Security Agency, with clear recommendations. The VFU will follow up on resolutions of adverse findings with the relevant P&SCM practitioner.

3.5.2 Procurement and Supply Chain Management:

The Procurement Manager responsible for the transaction must ensure that his/her procurement practitioner include adequate time for the security screening/vetting to be included in the project plan.

The Procurement Manager responsible for the transaction must ensure that his/her procurement practitioner enter the following clause as part of the Scope and for inclusion onto the Z Clauses, before tenders go out into the market for any security or related services:

> *"Acceptance of this tender is subject to the condition that both the contracting firm and its personnel providing the service must be security cleared by the appropriate authorities (Eskom vetting Fieldwork Unit & State Security Agency). Obtaining a positive recommendation is the responsibility of the contracting firm concerned. If the principal contractor appoints a subcontractor, the same provisions and measures will apply to the subcontractor.*
>
> *Acceptance of the tender is also subject to the condition that the contractor will implement all such security measures as the safe performance of the contract may require."*

The Procurement Manager must apply his/her mind to the recommendation from the relevant vetting authority State Security Agency (SSA) and VFU to ensure compliance with this directive and relevant legislation.

3.5.3 End-User/Security Manager:

The Security Manager must ensure there is written feedback from the relevant authority (SSA) and VFU before the start of the contract.

3.6 Process for Monitoring

The SSA is mandated to conduct security vetting and screening of service providers deployed at State owned entities, in line with the MISS and National Strategic Intelligence Act, 1994 (Act No 39 of 1994).

VFU in line with the extended mandate derived from the General Intelligence Laws Amendment Act 11 of 2013, and MoU signed by the Director General for the State Security Agency and Eskom Group Chief Executive is responsible for the implementation of security vetting and screening of service providers in conjunction with the SSA of throughout Eskom, its Divisions and Subsidiaries.

The VFU will monitor and report monthly to Risk and Governance Department on the compliance to this Directive taking into consideration requests for vetting or screening from P&SCM departments against security contracts in place.

4. Consequences of non-adherence to directive

All instances of non-compliance with this directive will be dealt with in terms of Eskom's Code of Conduct and may result in the possible suspension and or termination of such contract entered between Eskom and the third party.

5. Authorization

This document has been seen and accepted by:

Name	Designation
Tembela Kulu	General Manager Investigations and Security
Botse Sikhwitshi	Senior Manager Security Business Intelligence
Peter Malitsha	Senior Manager Security Investigations
Nomsa Spaumer	Senior Manager Security Business Enablement
Dr Remone Govender	Senior Manager Security Solutions Physical
Romeo Malgas	Middle Manager Vetting
Pilasande Qika	Middle Manager Security Business Intelligence
Ridwan Haffajee	Middle Manager Security Business Enablement
Monica Naidoo	Chief Advisor Business Enablement
Monette Roets	Middle Manager: Generation Security
Melvin Murugen	Middle Manager: NTCSA Security
Adolph Lekganyane	Middle Manager: Distribution Security
Samaria Mabona	Middle Manager: Eskom Real Estate Security
Motlhatlhani Khunou	Middle Manager: Risk Management Eskom Rotek Industries
Geoffrey Small	Middle Manager: NTCSA Project Delivery SHEQS
Ezekiel Thuntsane	Senior Manager: Procurement and Supply Chain Management
Maria Bowes	Senior Manager: Risk and Governance

6. Revisions

Date	Rev.	Remarks
January 2025	1	A business requirement identified in the company.

7. Development Team

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

Group Security (SBI, VFU, SBE, SI & SS)

8. Acknowledgements

The development team would like to thank all stakeholders for their valuable input throughout the drafting of this document.