Eskom	**Scope of Work**	**Group Investigations and Security**

Title: **Scope of work for a service to provide an independently managed live Fraud Hotline**

Document Identifier: **N/A**

Alternative Reference Number: **N/A**

Area of Applicability: **Eskom Holding and Subsidiaries**

Functional Area: **Forensic and Anti-Corruption**

Revision: **0**

Total Pages: **7**

Next Review Date: **Not Applicable**

Disclosure Classification: **Controlled Disclosure**

Compiled by

Daphne Morwalle
Chief Advisor: Forensic and Anti-Corruption

Date: 16 September 2025

Authorized by

Peter Malitsha
Senior Manager: Forensic and Anti-Corruption

Date: 23 Sep 2025

Content

Page

1. Introduction 3

3. Background information 3

4. General tender requirements 3

5. Eskom vetting requirements 6

1. Introduction

Eskom requires a service for an independently managed live Fraud Hotline providing for an anonymous reporting of known or suspected incidents of fraud, corruption, general crime, financial and general irregularities.

2. Background information

The Eskom Holdings is a state-owned company and a holding company. It comprises the operating company with its Subsidiaries and joint ventures. Eskom's core divisions, Generation and Distribution, rely on corporate support functions to operate effectively which include the Finance, Auditing, Strategic Delivery Unit, Renewable Energy Unit, Group Capital, Human Resources, Group Strategy and Sustainability, Group Investigations and Security, Company Secretary, Group Technology, and Group Corporate Services.
Eskom's current Subsidiaries include the National Transmission Company of South Africa SOC Ltd (NTCSA), Eskom Enterprises SOC Ltd (including Rotek Industries (ERI)), ESCAP SOC Ltd, Eskom Finance Company, and the Eskom Development Foundation.

Eskom's principal activity is the vertically integrated regulated electricity business that generates, transmits and distributes electricity to over 7 million customers across various segments including local industrial, mining, commercial, agriculture, redistributor (metropolitan and other municipalities), residential customers, and to international customers in southern Africa.
The electricity is generated by 30 power stations then transmitted over the transmission network and further distributed through an extensive distribution network that covers the entire country. Eskom's has over 40 thousand employees.

3. General Requirements

3.1 Company existence and experience profile

Existence of a company that provides hotline service (a service that provides a 24-hour live service to receive and register actual or suspected incidents of crimes and other irregularities including financial irregularities that are committed against the employer from employees, suppliers, customers and other stakeholders).

3.2 The nature of incidents

The nature of incidents includes crime (fraud, corruption, theft, vandalism, unethical conduct, irregularities including financial irregularities)

3.3 A commitment to protect whistleblowers / how Protection of Information Act is applied

3.4 Capacity (incident management system/tool)

Availability of a web-based tool with a repository that can be accessed by the employer to manage incidents that is supported by a secured technical infrastructure, encompassing hardware like computers, network equipment, software and related analytical tool/s, all managed through a reliable telecommunications network.

3.5 A web-based incident management system/tool with a platform that the Employer can access to manage the incident-related information.

Incident management system/tool with a repository that is supported by a secured technical infrastructure, encompassing hardware like computers, network equipment, software and related analytical tool/s, all managed through a reliable telecommunications network is in place/ web-based and can be accessed by the Employer.

3.6 Security of the facility/tool

A facility with appropriate security controls, backup systems, controlled access and audit trail dedicated to record keeping of all the incidents received for the duration of the contract and a minimum of 3 months after the expiry of the contract.

3.7 Operation of facility (incident management system/tool)

Capacity to take over the employer's toll-free telephone line within 24 hours of the contract, respond to live calls for 24 hours, 7 days a week, 365 days service.
Ability to answer calls and communicate with the callers in all 11 SA official languages
Capacity to establish additional reporting mechanisms dedicated to receiving confidential information on crime and irregularities including email account, SMS, WhatsApp, web-based.

An automated system to acknowledge receipt of reports that are received through the additional mechanisms

3.8 Management of incidents received on behalf of the employer

3.8.1 Receive and log reported incidents of crimes and other irregularities affecting the employer that includes the critical information from the caller, what happened, who did what happened, where did it happen, when did it happened, how did it happen and immediate allocation of a unique reference number of each call report in a sequential order that meets the employer's specific requirements.

3.8.2 Capacity to create categories and subcategories for the employer's approval of incidents received.

3.8.3 Capacity to create an independent report for each incident that can be downloaded and contains the following additional information:

3.8.3.1 The date the incident was received.

3.8.3.2 Incident category/type.

3.8.3.3 Full description of the incident.

3.8.3.4 Location where the incident occurred.

3.8.3.5 Unique incident reference number.

3.8.1.6 If not anonymous, the contact details of the reporter.

3.9 Capacity to create an independent report for each incident that can be downloaded and contains the information required under paragraph 3.8.3.

3.10 Accessibility f the records by the employer

Provision of a web-based facility that enables the employer to access and administer the recorded incidents 24/7, 7 days a week, 365 days of the year throughout the duration of the contract.

Capacity to enable the employer to access and download the recorded incidents individually and the entire database of incidents as an excel spreadsheet 24/7, 7 days a week, 365 days of the year throughout the duration of the contract.

A facility that keeps records and a copy of each incident submitted to the employer and make available such copy to the employer for the duration of the contract and three months after the expiry of the contract.

A facility that keeps records and a copy of each incident received on behalf of the employer and make available such copy to the employer for the duration of the contract and three months after the expiry of the contract.

A facility that allows the employer to download all the incidents received on its behalf through the mechanism including all the additional mechanisms

3.11 Communication of incidents and the statistics to the employer

Ability to isolate calls per the criteria specified by the employer and communicate such within a period of time stipulated by the employer to person/s nominated by the employer.

Ability to prepare and communicate reports of on-going crime immediately to a person/s designated by the employer followed by a comprehensive report within 24 hours of receiving the call from the reporter.

Ability to preparing and sending an on-going crime report to the designated individual or function as advised by the employer followed by a comprehensive report within 24 hours of receiving the call from the reporter.

Submitting a monthly summary report to the employer including all types of calls (dropped calls, testing call, concept query, prank calls) to the employer's designated recipient.

4. DUE DILIGENCE

4.1 Participating in this tender is subject to the screening of the company, directors and others assigned to provide the service.

- The screening will include the following areas:
  - Individual Criminal checks *(traffic offences excluded);*
  - Individual Qualification checks;
  - Individual Credits checks;
- Procurement checks:
  - CIPC;
  - SARS;
  - Property Information;
  - Restricted List, Legal Matter;
  - SAFPS;
  - Persal;
  - PEP; and
- All team members will also be required to sign Declaration of Secrecy (DoS).

4.2 Subcontractor Compliance

No subcontracting is allowed.

4.3 Consequence of non-compliance

- **Service provider:** Failure to comply with any material requirement above will result in the *"non-recommendation"* of the respective service provider for the project.
- **Service provider employees:** Failure to meet and or comply with any material requirement as listed above will result in the employee not being recommended for the

project (service provider may be allowed to provide a replacement resource with similar qualifications, experience, and capabilities).