



**Transmission Projects Delivery (TPD)  
Comprehensive Security Plan**

Title: **TPD Comprehensive Security Plan** Document Identifier: **TPDMAN-PN-119**

Alternative Reference Number: **N/A**

Area of Applicability: **Tx Projects Delivery**

Functional Area: **Security Management**

Revision: **1**

Total Pages: **26**

Next Review Date: **July 2026**

Disclosure Classification: **Controlled Disclosure**

**Compiled by**

*Nathan Kouter*

**Nathan Kouter  
Officer Security**

Date: 2022/08/04

**Supported by**

*Geoffrey Small*

**Geoffrey Small  
Middle Manager SHEQS**

Date: 04/08/2022

**Approved by**

*Naresh Singh*

**Naresh Singh  
General Manager**

Date: 04-08-22

**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.

## Content

### Page

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1	TPD SHEQS Operating Mandate .....	4
<b>2</b>	<b>DOCUMENT PURPOSE .....</b>	<b>4</b>
<b>3</b>	<b>AUTHORITY .....</b>	<b>4</b>
3.1	Accountability .....	4
3.2	Responsibility .....	4
3.3	Development and Implementation .....	5
<b>4</b>	<b>STATEMENT OF PURPOSE, KEY RESPONSIBILITIES AND DELIVERABLES .....</b>	<b>5</b>
4.1	Security Fraternity's Statement of Purpose .....	5
4.2	Key Processes .....	5
4.3	Key Responsibilities and Deliverables .....	5
<b>5</b>	<b>TPD SECURITY TEAM.....</b>	<b>6</b>
<b>6</b>	<b>SECURITY THREAT ASSESSMENT (STA).....</b>	<b>6</b>
<b>7</b>	<b>SECURITY PERSONNEL REQUIREMENTS .....</b>	<b>6</b>
<b>8</b>	<b>CONTRACTOR SECURITY REQUIREMENTS .....</b>	<b>6</b>
<b>9</b>	<b>SECURITY EQUIPMENT REQUIREMENTS .....</b>	<b>7</b>
<b>10</b>	<b>MONITORING OF SITE.....</b>	<b>7</b>
<b>11</b>	<b>ASSUMPTIONS.....</b>	<b>7</b>
<b>12</b>	<b>SECURITY RISKS (RISKS BELOW IS NOT EXHAUSTIVE).....</b>	<b>7</b>
<b>13</b>	<b>CONSTRAINTS .....</b>	<b>8</b>
<b>14</b>	<b>ROLES AND RESPONSIBILITIES.....</b>	<b>8</b>
<b>15</b>	<b>REFERENCES.....</b>	<b>9</b>
<b>16</b>	<b>DOCUMENT ACKNOWLEDGEMENT .....</b>	<b>9</b>

### 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>ANNEXURES .....</b>	<b>10</b>
<b>A.1 CONTINGENCY PLANNING SCENARIOS AND ASSUMPTIONS.....</b>	<b>10</b>
<b>A.2 RESPONSE OBJECTIVES .....</b>	<b>11</b>
<b>A.3 SECURITY ALERT LEVELS .....</b>	<b>11</b>
<b>A.3 ACTIVE RESPONSE .....</b>	<b>14</b>
<b>A.4 PLANNED SCENARIOS, ASSUMPTIONS AND SECURITY RESPONSE .....</b>	<b>15</b>
<b>A.5 ACTUAL SCENARIO IN A CRIME SITUATION USING CONTRACT SECURITY .....</b>	<b>18</b>
<b>A.5.1 TYPICAL SECURITY PLAN.....</b>	<b>18</b>
<b>A.6 EMERGENCY ESCALATION PROCESS WITHIN ESKOM FOR SECURITY .....</b>	<b>21</b>
<b>A.6.1 INTERNAL EMERGENCY STRUCTURES OR ROLE PLAYERS .....</b>	<b>21</b>
<b>A.6.2 EXTERNAL EMERGENCY STRUCTURES/RESPONSE PARTNERS.....</b>	<b>23</b>
<b>A.6.3 INCIDENT MANAGEMENT WORKFLOW .....</b>	<b>26</b>

**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

### 1.1 TPD SHEQS Operating Mandate

TPD SHEQS's mandate is to "integrate and oversee sustainable performance and services in the fields of construction occupational health and safety & occupational hygiene, environmental, quality & security management to strive for Zero Harm to people, plant, and the environment, and Zero defects in the quality of our execution."

The security function is critical to the organization's legal compliance and risk management; therefore, it is critical to align with the business goals and strategies that affect TDP employees and assets.

## 2 DOCUMENT PURPOSE

This plan serves as the foundation for measuring the project's site security activities. To embrace the fundamental key security principles of deterrence, detection, delay, and response, it is possible to clearly identify and specify security personnel requirements, legislative and regulatory requirements for a project.

## 3 AUTHORITY

### 3.1 Accountability

The following individuals are accountable for the security of TPD:

When there are no National Key Point areas on the site:	General Manager – TPD
When a location is designated as a National Key Point:	General Manager – Grids

### 3.2 Responsibility

The following individuals are responsible for the site security:

When there are no National Key Point areas on the site:	Project Manager – Portfolios
When a location is designated as a National Key Point:	Senior Manager – Grids

According to the NEC, the Project Manager is also responsible for:

- managing the project's day-to-day activities, including security management;
- resource allocation, and team motivation and delivery.

**Note:** The Project Manager should include Security Requirements in the Works Information.

### 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 Development and Implementation

The following positions are responsible for developing and implementing security plan:

Before any area is designated as a National Key Point; green/brown field line servitude(s)	TPD Security Manager /Senior Advisor/Officer
Following the designation of any location as a National Key Point	Grids Security Manager

## 4 STATEMENT OF PURPOSE, KEY RESPONSIBILITIES AND DELIVERABLES

### 4.1 Security Fraternity's Statement of Purpose

To provide security advice, Security Threat Assessment (STA), security oversight, and security solution coordination in TPD.

### 4.2 Key Processes

- Consultation and communication;
- Context setting;
- Problem definition;
- Interpreting threat and Risk Assessments;
- Assessing the effectiveness of existing controls (vulnerability studies);
- Adversary and tactic analysis;
- Development of security controls and measures;
- User specifications and technical standards;
- Assurance and Governance.

### 4.3 Key Responsibilities and Deliverables

- Create security solutions and draft minimum security standards in accordance with legal and regulatory requirements;
- Define security system requirements to address identified and emerging security threats and risks;
- Conduct and initiate research initiatives to identify and select suitable security solutions;
- Direct and coordinate the implementation of Physical Security solutions in TPD;
- Maintain regular communication with Project Managers, Contractors, and Security Service Providers;
- Continuous environmental scanning that will monitor and address violence against the project assets and employees
- Raising security awareness and fostering a pro-security culture.

#### **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 TPD SECURITY TEAM

Name	Role	Contact Details	Portfolios
Nathan Kouter	Officer Security	KouterN@eskom.co.za 011 – 800 2826 060 537 5970	<ul style="list-style-type: none"><li>• Gauteng Portfolio</li><li>• Mpumalanga Portfolio</li><li>• Northern Portfolio (Northwest &amp; Limpopo)</li></ul>
Noel Smouse	Officer Security	SmouseND@eskom.co.za 011 – 800 2946 079 503 3719	<ul style="list-style-type: none"><li>• KwaZulu-Natal Portfolio</li><li>• Southern Portfolio (Free State &amp; Eastern Cape)</li><li>• Western Portfolio (Western &amp; Northern Cape)</li></ul>

## 6 SECURITY THREAT ASSESSMENT (STA)

The STA methodology makes use of security discipline methods to study and analyse the identified threats (cause/ source to a risk), controls and treatments associated with.

Example of such methods:

- Environmental scanning
- Vulnerability study
- Impact analysis study (*Consequence*)
- Cost benefit analysis
- Likelihood study (*Probability*)

## 7 SECURITY PERSONNEL REQUIREMENTS

All security personnel must meet PSIRA and project-specific security scope of work (SOW) requirements.

## 8 CONTRACTOR SECURITY REQUIREMENTS

To ascertain compliance with PSIRA requirements and project-specific security scope of work (SOW) applicable to the project, as well as its implementation and effectiveness:

- Evaluate the contractor's adherence to the PSIRA requirements and project SOW;
- Valid COIDA;
- Valid Medicals [Certificate of Fitness (COF's)];
- Security service providers – Project Risk Assessments;
- Security service providers – Project Security Plans;

**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.

- Security service providers – Technical evaluations including mandatory requirements;
- Security service providers and Contractor Employees – Criminal Records (valid for 12months, before commencement of work at Eskom sites and Servitudes);
- Monitoring the execution of all access control steps to ensure consistency and compliance with Eskom security and other requirement.

## 9 SECURITY EQUIPMENT REQUIREMENTS

The following security equipment is for projects or sites, but it is not exhaustive:

Standard / Procedure	Document Number
Standard for Bullet-resistant Guard facilities	240-91252315
Physical Access Control at Eskom Premises	32-1134
Specification for Non-Lethal Energized Perimeter Detection Systems	240-78980848
Specification for Integrated Access Control System for Eskom Sites	240-102220945
Lighting for perimeter security at Eskom installations	240-91252455
Specification For CCTV Surveillance with Intruder Detection	240-91190304

## 10 MONITORING OF SITE

The following will monitor sites to ensure a safe and secure site environment:

- Physical and static guarding, as well as foot patrols
- Armed response
- K9 Services
- Services for escorting and monitoring
- Tactical Response Services.

## 11 ASSUMPTIONS

Annexure 1 contains a list of assumptions.

## 12 SECURITY RISKS (risks below is not exhaustive)

No	Risk Area / Threat	Likelihood	Risk Owner	Impact-Mitigation Plan
1	TPD Projects & Sites	High	Project Manager	STA
2	Environmental scanning of conditions	High	Project Manager	SOW / STA
3	Community Protest	High	Project Manager	TPD Comprehensive Security Plan
4	Theft	High	Project Manager	TPD Comprehensive Security Plan
5	Intimidation	High	Project Manager	TPD Comprehensive Security Plan

### 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.

### 13 CONSTRAINTS

The following constraints, both internal and external to a Project, will have an impact on site security:

- Budgets for projects
- A scarcity of qualified and experienced security service providers

### 14 ROLES AND RESPONSIBILITIES

Activity No	Process Step/Activity Description	Project Manager	Site Manager/Site Representative	Stakeholder Management	Contractor Management	Security Management (Contractor)	Security Management (Client)	Required for the Project
1	Security requirements in the Works Information	R	R	I	I	I	C	M
2	Site Security Threat Assessment	R	I	I	R	I	R	M
3	Operational Security	R	C	-	R	R	C	M
4	Reporting and investigating of crime incidents	R	I	I	R	R	R	M
5	Community related issues/ Threat / Instability /Intimidation reports from various sites	R	I	R	R	C	C	M

#### 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.



## 15 REFERENCES

Description	Document Number
National Industrial Action - Disaster Contingency Plan	240-123324469
Security Threat Assessment (STA) Standard	240-79537982
TPD Scope of Work (SOW)	Project Specific
Construction Regulations Audit Checklist	240-180000215
National Strategic Intelligence Act	Act No. 39 of 1994
The Critical Infrastructure Protection	Act No. 8 of 2019

## 16 DOCUMENT ACKNOWLEDGEMENT

Noel Smouse – Officer Security

Bongani Mabena – Manager Occupational Health & Safety

Julie Cheerkoot – Middle Manager: Security Operations

Ntombekhaya (Ntosh) Mafumbatha – External Stability 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.

## ANNEXURES

### A.1 Contingency Planning Scenarios and Assumptions

Based on the Security Treat Assessment (STA) conducted, the following scenarios and related assumptions are considered in the plan.

**Table 1: Planning Scenarios**

No	Scenario Name	Description/Assumptions
A	Business Unit Protest	Independent BU protests (transporting of employees to Eskom facilities to increase protest numbers)
B	Picketing	Unannounced picketing and sit-ins within the Eskom boundaries
C	Blockading at Eskom facility or servitudes	Blockading of Eskom facility main entrance and access points, including servitudes thereby impacting employee accessibility, especially critical/scarce-skill employees and emergency vehicles
D	Contract security protest	Contract security participating in industrial action
E	Unauthorised entry	Plant tampering, Sabotage, Vandalism, Malicious damage to property of critical infrastructure / sabotage of security systems
F	Protest action between various	Planned collective protest action between BUs, permanent contractors and surrounding communities
G	Hijacking	Hi-jacking of Eskom or Contractor vehicle
H	Intimidation	Intimidation of employees or contractors
I	Road blockade	Blockading of public roads

#### 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.

## A.2 Response Objectives

**Table 2: Objectives & Description**

No	Objective	Description
1	Safeguarding of employees and contractors including strikers	Protect the employees and striking employees
2	Safeguarding of Eskom infrastructure	Protect the critical infrastructure from theft, malicious damage to property and sabotage

## A.3 Security Alert Levels

**Table 3: Alert Levels**

Alert level	Description of threat condition	Description of minimum-security measures	Objectives	Activation of Security Support Structures
<b>Level 1</b> (Normal Operations)	Normal operations	Normal operating environment. <ul style="list-style-type: none"><li>• Baseline security measures implemented</li><li>• Regulatory compliance ensured</li><li>• Specific organisational requirements met (risk based)</li></ul>	<ul style="list-style-type: none"><li>• Control the movement of people and assets on, in and out of site</li><li>• Maintain security awareness and systems for the reporting of anything suspicious activity/object</li><li>• Maintain response / assistance capacity</li></ul>	None

### 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>Level 2</b> (Significant threat)	Specific and significant threat against the organisation, its assets, people and operations	<p>Security measures for Level 1 applicable.</p> <p>Additional controls to address the specific threat:-</p> <ul style="list-style-type: none"> <li>Identify and deny adversaries access.</li> <li>Additional security measures at identified vulnerable points to deter, detect, delay, report, respond and recover.</li> </ul>	<p>Limit movement on, to and from site as appropriate</p> <ul style="list-style-type: none"> <li>Additional screening on visitors done beforehand</li> <li>Improved screening of deliveries.</li> <li>Denial of access to specific areas as appropriate (zoning).</li> <li>Domination of environment</li> <li>Increase security deployment</li> </ul>	<ul style="list-style-type: none"> <li>Continuous communication with local SAPS and emergency services</li> <li>Site emergency response team and JOC on standby.</li> <li>Increase deterrence, detection, delay and response capacity</li> </ul>
<b>Level 3</b> (High threat level)	Credible and imminent threat	<ul style="list-style-type: none"> <li>Security measures for Level 2 applicable.</li> <li>Restricted access and egress essential to all personnel (Eskom employees and contractor)</li> <li>No visitors allowed on site</li> </ul>	<p>Limit and closely monitor people on site, with the view to prevent harm to assets, information, interests, people and processes</p> <p>Limit access and egress transactions as well as movement on site</p>	<p>The following emergency structures must be activated:-</p> <ul style="list-style-type: none"> <li>ERCC, JOCs and PJCCs.</li> <li>Relevant support/reaction forces deployed</li> </ul>

### 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.

		<ul style="list-style-type: none"> <li>Constant monitoring of all security systems</li> <li>Only essential deliveries or removal from site allowed</li> </ul>		
<b>Level 4</b> (Under attack)	Actual attack or Incident	<p>Security measures for Level 3 applicable.</p> <ul style="list-style-type: none"> <li>Lock down or partially lockdown of installation / facility / substation (subject to decision by ERCC)</li> <li>Execute emergency response and contingency plans</li> <li>All available security members must be on site</li> </ul> <p><b>Site security to be supported by law Enforcement Agencies (SAPS, SANDF, SSA)</b></p>	<p>Limit harm to assets, information, interests, people and processes. Facilitate recovery.</p>	<p>The following emergency structures must be activated:- ERCC, JOCs and PJCCs.</p>

### 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.

### A.3 Active Response

**Table 4: Invoking the Response Plan**

Anticipate / Adapt	Assess & Operate	Activate response	Recover	Learn / Evolve
<ul style="list-style-type: none"> <li>Receive incident notification</li> <li>Inform Security Management</li> </ul>	<ul style="list-style-type: none"> <li>Conduct situational assessment</li> <li>Move site to appropriate security alert level</li> <li>Determine required security support for site and employees</li> <li>Deploy security personnel to the critical site(s)</li> <li>Secure site until SAPS is deployed.</li> </ul>	<ul style="list-style-type: none"> <li>Inform SAPS Cluster commander</li> <li>Identify response required, resources needed.</li> <li>Determine all security requirements from the Division.</li> <li>Security Division TCC advises site(s) of Tactical Response Plan.</li> </ul>	<ul style="list-style-type: none"> <li>Monitor and give continuous support to project management and site security for as long as required.</li> <li>Maintain security update to Management.</li> <li>Monitor and support security agencies (SAPS)</li> <li>Resolve any constraints, escalate issues and engage with stakeholders.</li> <li>Maintain ongoing situation awareness until normal operations is confirmed.</li> </ul>	<ul style="list-style-type: none"> <li>Post incident reporting to Management</li> <li>Debriefing</li> <li>Stakeholder relationship</li> <li>Reporting:- Close-out report – lessons learnt, actions taken, what worked, what did not work.</li> <li>Post incident investigations</li> <li>Resumption of business operations</li> <li>Emergency response evaluations &amp; post incident reviews</li> <li>Employee assistance</li> <li>Review security plan based on lessons learnt.</li> </ul>

**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.

## A.4 Planned Scenarios, Assumptions and Security Response

Table 5: Management &amp; Security Response

Scenario description / Assumption	Impact	Security Response	Management Response
<ul style="list-style-type: none"> <li>Independent BU protests (transporting of employees to Eskom facilities to increase protest numbers)</li> </ul>	<ul style="list-style-type: none"> <li>Disruption of services and production/ business operations</li> <li>Violence and intimidation</li> <li>Fatalities</li> <li>Damage to property</li> <li>Road blockages and blockages of access points</li> </ul>	<ul style="list-style-type: none"> <li>Shut down access to site</li> <li>Activate appropriate security alert level emanating from the threat</li> <li>Law enforcement agencies must be notified of the strike action.</li> <li>Security Manager execute Industrial action plans, Security Plans and contingencies</li> <li>Safeguarding and protection of Management team during receipt of memorandum.</li> <li>Remove obstructions and deploy guards at access control points and other vulnerable areas.</li> <li>Increase security patrols and visibility at critical plant zones</li> <li>Ensure no use of Eskom assets by strikers.</li> </ul>	<ul style="list-style-type: none"> <li>Identify leaders for possible negotiations sessions</li> <li>Establish the demands of strikers and convey to EP team and Eskom management</li> <li>Ensure Stakeholder management is involved during the memo handover.</li> <li>Notify external emergency personnel and response companies.</li> <li>Management to activate Security service providers to be used to supplement manpower shortages</li> <li>Deploy TRT to conduct first line crowd control measures</li> </ul>
<ul style="list-style-type: none"> <li>Unannounced picketing and sit-ins within the Eskom boundaries</li> </ul>	<ul style="list-style-type: none"> <li>Disruption of service &amp; operations</li> </ul>	<ul style="list-style-type: none"> <li>Activate strike contingency plans</li> <li>Initial interventions by security must be</li> </ul>	<ul style="list-style-type: none"> <li>Management to provide feedback to Security Tactical</li> </ul>

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.

	<ul style="list-style-type: none"> <li>• Road blockages</li> <li>• Employee safety</li> <li>• Vandalism &amp; damage to property</li> <li>• Burning of vehicles</li> <li>• Field fires around sites</li> <li>• Intimidation and prevention of key personnel providing essential services</li> </ul>	executed in a manner that does not provoke striking employees <ul style="list-style-type: none"> <li>• Increase security alert levels</li> <li>• Local SAPS to be notified of the protest action</li> <li>• Security Manager to execute Site Security Plans and contingencies</li> <li>• Increase security patrols and visibility at critical plant zones</li> <li>• Security to assess the situation</li> </ul>	Command Centre (TCC) in Division
<ul style="list-style-type: none"> <li>• Blockading of Eskom facility main entrance and access points, including servitudes thereby impacting employee accessibility, especially critical/scarcely-skill employees and emergency vehicles</li> </ul>	<ul style="list-style-type: none"> <li>• Unavailability of critical staff to ensure the continuation of operations and service delivery</li> <li>• Emergency services cannot access the site</li> </ul>	<ul style="list-style-type: none"> <li>• Security manager to activate appropriate security alert level</li> <li>• Activate strike contingency site plan</li> <li>• Security to assess the situation and provide feedback to management.</li> <li>• Security Manager contacts local SAPS</li> <li>• SAPS/Traffic department to control and re-direct traffic.</li> </ul>	<ul style="list-style-type: none"> <li>• Management to provide feedback to Security Tactical Command Centre (TCC) in Division</li> <li>• Management will source and deploy tactical response capabilities to assist site</li> </ul>
<ul style="list-style-type: none"> <li>• Contract security participating in industrial action</li> </ul>	<ul style="list-style-type: none"> <li>• Inadequate security numbers to secure NKP and other sites</li> <li>• Uncontrolled access</li> </ul>	<ul style="list-style-type: none"> <li>• Lock down site</li> </ul>	<ul style="list-style-type: none"> <li>• Management to deploy TRT for additional resources Engage contract IR/HR</li> </ul>
<ul style="list-style-type: none"> <li>• Unauthorised entry Plant tampering,</li> </ul>	<ul style="list-style-type: none"> <li>• Damage to property</li> </ul>	<ul style="list-style-type: none"> <li>• Proactive deployment of</li> </ul>	<ul style="list-style-type: none"> <li>• Maintains communication</li> </ul>

**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.



Sabotage, Vandalism, Malicious damage to property of critical areas of the plant / sabotage of security systems	<ul style="list-style-type: none"> <li>• Destruction of operations</li> </ul>	guards to red zones, critical and affected areas <ul style="list-style-type: none"> <li>• Ensure CCTV coverage</li> <li>• Arrest suspects</li> <li>• Open a criminal case with SAPS</li> <li>• Investigate incidents</li> </ul>	with high level Management and Local Authorities <ul style="list-style-type: none"> <li>• Takes the necessary actions in co-operation with the Security Manager</li> <li>• To be part of JOC</li> <li>• Continuous Press statements if necessary</li> </ul>
<ul style="list-style-type: none"> <li>• Planned collective protest action between BUs, permanent contractors and surrounding communities</li> </ul>	<ul style="list-style-type: none"> <li>• Disruption of services and operations</li> </ul>	<ul style="list-style-type: none"> <li>• Increase security alert levels</li> <li>• Inform SAPS</li> </ul>	<ul style="list-style-type: none"> <li>• Management to deploy TRT for additional resources</li> <li>• Inform Divisional TCC and ERCC</li> </ul>
<ul style="list-style-type: none"> <li>• Hi-jacking of Eskom or Contractor vehicle</li> </ul>	<ul style="list-style-type: none"> <li>• Delayed operations</li> </ul>	<ul style="list-style-type: none"> <li>• Inform Management</li> <li>• Inform SAPS</li> <li>• Investigate the incidents</li> </ul>	<ul style="list-style-type: none"> <li>• Maintains communication with high level Management and Local Authorities</li> </ul>
<ul style="list-style-type: none"> <li>• Intimidation of employees or contractors</li> </ul>	<ul style="list-style-type: none"> <li>• Employees not reporting for duty</li> <li>• Delayed operations</li> </ul>	<ul style="list-style-type: none"> <li>• Inform Management</li> <li>• Inform SAPS</li> <li>• Investigate the incidents</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure Stakeholder management is involved</li> <li>• Management to deploy TRT for support</li> <li>• Maintains communication with high level Management and Local Authorities</li> </ul>
<ul style="list-style-type: none"> <li>• Blockading of public roads</li> </ul>	<ul style="list-style-type: none"> <li>• Employees unable to report for duty</li> </ul>	<ul style="list-style-type: none"> <li>• Inform SAPS</li> <li>• Request support from SAPS to divert traffic and clearing of roads</li> </ul>	<ul style="list-style-type: none"> <li>• Management to deploy TRT for support</li> <li>• Maintains communication with high level Management and Local Authorities</li> </ul>

**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.

## **A.5 Actual Scenario in a Crime Situation Using Contract Security**

### **A.5.1 Typical Security Plan**

Unauthorised entry into the Substation or HV Yard through or underneath the Perimeter and electric fences or through the access gate under false pretence or on the Eskom servitude with the purpose / intent to commit any crime.

#### **Purpose**

- Establish extent and nature of the situation
- Establish severity of situation
- To ensure rapid response from the SAPS and SAPS Task Force
- To normalise the situation as soon as possible

#### **Decisions / Actions**

- Obtain so much information as possible
- To notify all important role-players as needed
- To determine the actions needed to prevent loss of life / injuries
- To enhance the protection and safety of employees / valuables
- Determine enemy's ability

#### **Disciplines Involved**

- Security Guards
- Contract Provider Control room
- Contract Security Manager
- Project Manager (Contractor)
- Project Manager (Client)
- Security Management (Client)
- South African Police and Task force

**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>Transmission Projects Delivery (TPD) Comprehensive Security Plan</b>	
---	---	--

**Table 6: Security Plan for a Crime Situation E.g., Theft of Steel or Damage to Critical Infrastructure**

<b>Observer</b>	<b>Security Guard(s)</b>	<b>Contract Security Manager</b>	<b>Project Manager (Contractor)</b>	<b>Security Management (Client)</b>	<b>Project Management (Client)</b>
<ul style="list-style-type: none"> <li>• Reports and alerts security</li> <li>• Takes cover and maintains observation</li> <li>• Reports any casualties</li> <li>• Maintains communication</li> <li>• Be available for investigation</li> </ul>	<ul style="list-style-type: none"> <li>• Receives information or perceives</li> <li>• Takes cover and be vigilant</li> <li>• Press panic button immediately</li> <li>• Returns fire if possible and necessary</li> <li>• Notifies Colleague (s)</li> <li>• Obtains all information if possible</li> <li>• Notifies and brief Contract Provider Control room</li> </ul>	<ul style="list-style-type: none"> <li>• Receives information</li> <li>• Informs Management</li> <li>• Informs SAPS and other Emergency services</li> <li>• Arranges for reinforcement</li> <li>• Increase patrol and access control duties and be vigilant. Do not open the gate or admits any people on site.</li> </ul>	<ul style="list-style-type: none"> <li>• Receives information</li> <li>• Evaluates situation</li> <li>• Notifies and brief Contractors Management &amp; Client Project Manager</li> <li>• Proceeds to scene and evaluates situation and assess risk – severity of situation</li> <li>• Establish if any casualties</li> </ul>	<ul style="list-style-type: none"> <li>• Receives information</li> <li>• Evaluates situation</li> <li>• Notifies and brief Management as necessary</li> <li>• Proceeds to scene and evaluates situation and assess risk – severity of situation</li> <li>• Consults with SAPS and other Emergency Services</li> <li>• Regular feedback to JOC</li> </ul>	<ul style="list-style-type: none"> <li>• Receives information</li> <li>• Maintains communication with high level Management and Local Authorities</li> <li>• Takes the necessary actions in co-operation with the Security Manager</li> <li>• To be part of JOC</li> <li>• Continuous Press statements if necessary</li> </ul>

**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.

	<ul style="list-style-type: none"> <li>• Reports any casualties</li> <li>• Evacuates substation if possible</li> <li>• Increase patrol and access control duties and be vigilant. Do not open the gate or admits any people on site.</li> <li>• Maintains communication</li> <li>• Record keeping (OB and pocket book)</li> </ul>	<ul style="list-style-type: none"> <li>• Maintains communication</li> <li>• Acts on instructions / requests</li> <li>• Barricades scene of crime</li> <li>• Access Control – Nobody admits into site</li> <li>• Notifies and brief Management of results and advice</li> <li>• Initiates JOC and notifies JPC members</li> </ul>	<ul style="list-style-type: none"> <li>• Establish whether all Emergency services were informed</li> <li>• To be part of JOC</li> </ul>	<ul style="list-style-type: none"> <li>• Awaiting information of SAPS</li> <li>• Conducts investigation</li> <li>• Pre-liminary report to NKP Commander</li> <li>• After investigation submit final report to NKP Commander</li> <li>• Re-evaluation of the Security measurements in place and protection of the site.</li> </ul>	<ul style="list-style-type: none"> <li>• Regular feedback to employees and role-players</li> </ul>
--	---	--	---	---	--

**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>Transmission Projects Delivery (TPD) Comprehensive Security Plan</b>	
---	---	--

## A.6 Emergency Escalation Process within Eskom for Security

### A.6.1 Internal Emergency Structures or Role Players

No	Internal Role Player	What	By who	To who	When	How
1	<b>Site Security</b>	<p>The construction site's assets are protected and safeguarded by a security service provider that the contractor hires; riot control and other community issues are not the responsibility of the security service provider. A tactical response agreement is established for a brief period in tense situations (volatile areas).</p> <p><b><u>Note: The Eskom escalation process is outlined below.</u></b></p>	Security Manager/ Supervisor	Project Management, TPD Security Management	Within 10 Minutes of incident	Telephone

### 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	<b>Divisional Security</b>	Threat / Instability /Intimidation reports from various sites	Divisional Security Manager	Security TCC Chairperson	Within 30 minutes of incident	Telephone
3	<b>Security TCC</b>	Threat / Instability reports from divisional security managers	Security TCC Chairperson	GM Security ERCC Chairperson	Within 45 Minutes of incident	Telephone
4	<b>ERCC</b>	Instability reports from Security TCC	ERCC Chairperson	GCE	Within 1 hour of the incident	Telephone
5	<b>GCE</b>	Organisational instability reports	GCE	DPE, DoE, NATJOINTS	within 2 minutes of the	Telephone

**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.

### A.6.2 External Emergency Structures/Response Partners

No.	Notification or Activation					Deactivation/Demobilization			
	Response partner	Responsible	Trigger	Trigger level	Time frame	Responsible	Trigger	Trigger level	Timeframe
1	<b>SSA</b>	Senior Manager: Security Business Intelligence	Instability/Intimidation/ Protest actions hampering normal operations at projects / sites	Security Business Intelligence GM Security Security TCC Chairperson	Within 30 minutes of incident	General Manager: Security	Normal operations in sites	Security Business Intelligence GM Security Security TCC Chairperson	Within 24 hours after the incident
2	<b>SAPS Station or - District SAPS</b>	Security Manager / Site Manager	Instability/Intimidation/Protest actions hampering normal operations at projects / sites	Site Security Manager Divisional Security Manager GM Security Security TCC Chairperson	Within 15 minutes of incident	Site Security / JOC	Normal operations in Eskom sites	Site Security Manager Divisional Security Manager GM Security	Within 24 hours after the incidents

**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.

No.	Notification or Activation					Deactivation/Demobilization			
	Response partner	Responsible	Trigger	Trigger level	Time frame	Responsible	Trigger	Trigger level	Timeframe
								Security TCC Chairperson	
3	<b>PROVJOINTS</b>	Divisional Security Manager	Instability/Intimidation/Protest actions hampering normal operations at projects / sites	Site Security Manager Divisional Security Manager	Within 1 hour of incident	Divisional Security Manager	Normal operations in sites	Site Security Manager Divisional Security Manager	Within 24 hours after the incident
4	<b>NATJOINTS</b>	General Manager: Security	<ul style="list-style-type: none"> <li>• Instability/Intimidation/Protest actions hampering normal operations at projects / sites</li> <li>• Eskom technicians unable to attend to faults.</li> <li>• Information from site security</li> </ul>	GCE ERCC PJCC, PROVJOINTS, NATJOINTS NDMC	Within 1 hour of ERCC Initial Briefing	General Manager Security	Normal operations in Eskom sites	GCE ERCC PJCC, PROVJOINTS, NATJOINTS NDMC	Within 24 hours after the incidents

**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.



**External Emergency Support for existing projects**

- SAPS - workflow process once triggered by Eskom (action plan)
- SAPS i.t.o. response turnaround time
- SAPS escalation points
- Clarification of the SAPS's function and role upon arrival at the incident scene
- Instruction from Provjoints to SAPS station commanders in problematic municipalities to support Eskom

**Support required for medium/long term projects**

- Visible policing
- Allocation of a dedicated SAPS team to patrol site at agreed intervals
- Attendance at strategic meetings E.g. Programme Managers, Project Managers, etc.

**Note:**

TCC – Tactical Command Centre

ERCC – Emergency Response Command Centre

NKP – National Key Point

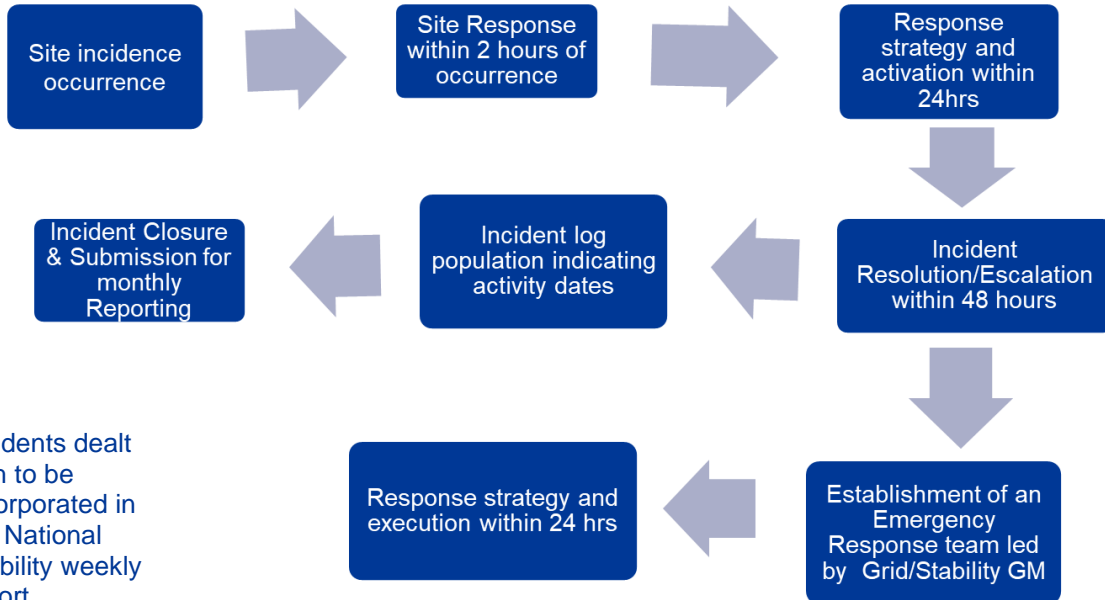
JOC – Joint Operation Centre

**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.

### A.6.3 Incident Management Workflow



- Incidents dealt with to be incorporated in the National Stability weekly report
- Incidents to be tabled in integration meetings for collaboration and resolution.

- Incident developments to include:**
- Alert to Eskom, SAPS, Municipality, COGTA rapid response team
  - Development of the Incident Briefing Note
  - Preparation of Media Holding Statement

**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.