STANDARD OPERATING PROCEDURE (SOP)

ESKOM MKONDENI SECURITY CONTROL ROOM OPERATIONS

Document Title: Standard Operating Procedure for the Operation of the Eskom Mkondeni Security Control Room
Location: Eskom Mkondeni Control Room, KwaZulu-Natal
Department: Security Risk Management
Effective Date: _____
Review Date: _____
Version: 1.0

1. PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to establish uniform operational standards for the management and operation of the Eskom Mkondeni Security Control Room. The Control Room serves as the centralized security monitoring and incident management centre responsible for real-time surveillance, alarm monitoring, communication, incident coordination, reporting, and intelligence-driven security decision-making across Eskom facilities and infrastructure linked to the Control Room. The SOP incorporates centralized monitoring, video wall technology, automated reporting, secure communications, and compliance with the Protection of Personal Information Act (POPIA).

---

2. SCOPE

This SOP applies to:

- Security Control Room Operators
- Control Room Supervisors
- Security Risk Manager
- Armed Response Providers
- Security Service Providers
- Eskom Security Personnel
- Technical Support Personnel
- Contractors responsible for CCTV, alarms, access control, communications, and analytics systems

The SOP governs all security systems integrated into the Eskom Mkondeni Security Control Room, including:

- CCTV Systems
- Intrusion Detection Systems
- Access Control Systems
- Video Analytics
- AI-Based Threat Detection Systems
- Alarm Monitoring Platforms
- Communication Networks
- Incident Management Systems
- Automated Reporting Platforms

---

3. CONTROL ROOM OBJECTIVES

The Control Room shall:

1. Provide 24-hour continuous monitoring of Eskom sites.
2. Detect, verify, and respond to security incidents in real time.
3. Coordinate emergency and armed response resources.
4. Provide centralized visibility across multiple Eskom facilities.
5. Generate automated incident reports and management dashboards.
6. Improve situational awareness and proactive security management.
7. Ensure compliance with Eskom security policies and POPIA requirements.
8. Support business continuity through resilient technology infrastructure.

4. CONTROL ROOM INFRASTRUCTURE

The Control Room shall be equipped with:

4.1 Video Wall

A state-of-the-art video wall shall display:

- Live CCTV feeds
- Alarm events
- Perimeter intrusion alerts
- Access control exceptions
- AI analytics notifications
- Incident maps and dashboards
- Site operational status

The video wall shall operate continuously and provide operators with real-time situational awareness.

4.2 Communication Systems

The Control Room shall utilize secure high-speed communication networks incorporating:

- Fibre-based connectivity
- Encrypted data transmission
- Radio communication systems
- VoIP communication systems
- Cellular backup communication channels
- Secure communication links to field operations

Communication systems shall support uninterrupted operational coordination between the Control Room and field personnel.

4.3 Security Management Platform

The centralized platform shall integrate:

- CCTV
- Alarms
- Access Control
- Analytics
- Incident Reporting
- Dispatch Services
- Audit Logs

All systems shall be integrated into a single monitoring environment wherever feasible.

5. CONTROL ROOM STAFFING

The Control Room shall operate 24 hours per day, 7 days per week.

Minimum Shift Personnel

Position	Responsibility
Control Room Operator	Monitoring and incident management
Senior Operator	Escalation and coordination
Control Room Supervisor	Shift oversight and decision-making
Technical Support (on-call)	System support and maintenance

Shift Structure

- Day Shift: 06:00–18:00
- ~~Afternoon~~Night Shift: 1[1]8:00–~~22~~06:00

A formal handover shall take place at the start and end of every shift.

6. CCTV MONITORING PROCEDURES

Operators shall:

Continuous Monitoring

- Monitor live feeds at all times.
- Prioritize critical infrastructure sites.
- Monitor perimeter security systems continuously.
- Maintain active video verification capability.

Suspicious Activity Detection

The following shall be immediately investigated:

- Unauthorized persons
- Forced entry attempts
- Loitering
- Vehicle abnormalities
- Vandalism
- Theft-related activities
- Cable theft indicators
- Tampering with infrastructure

Incident Verification

Upon receiving an alert:

1. Access associated camera feeds.
2. Verify alarm authenticity.
3. Capture screenshots/video evidence.
4. Notify the Supervisor.
5. Dispatch response resources.
6. Record actions on the incident management system.

7. ALARM MONITORING PROCEDURES

All alarms shall receive immediate attention.

Alarm Categories

Priority 1

- Intrusion alarms
- Panic alarms
- Fire alarms
- Critical infrastructure breaches

Priority 2

- Access control exceptions
- Perimeter disturbances
- Equipment tampering

Priority 3

- System faults
- Communication failures

Alarm Response

The operator shall:

1. Acknowledge alarm.
2. Verify through CCTV.
3. Contact site personnel where applicable.
4. Dispatch response services.
5. Escalate to Supervisor.
6. Record incident reference number.

8. INCIDENT MANAGEMENT

All incidents shall be managed in accordance with Eskom Security Incident Management Processes.

Incident Categories

- Theft
- Cable theft
- Vandalism
- Illegal connections
- Intrusion
- Protest action
- Fire

- Medical Emergency
- Suspicious Activity
- System Failure

Incident Management Process

1. Detection
2. Verification
3. Classification
4. Escalation
5. Response Coordination
6. Documentation
7. Closure
8. Reporting

9. COMMUNICATIONS AND ESCALATION

The Control Room shall serve as the primary communication hub.

Escalation Levels

Level 1

Control Room Operator

Level 2

Control Room Supervisor

Level 3

Security Management

Level 4

Emergency Services / SAPS / Armed Response

Communication Requirements

All communication shall be:

- Accurate
- Professional
- Recorded where applicable
- Logged in the Incident Management System

10. AUTOMATED REPORTING AND ANALYTICS

The system shall generate automated reports for proactive threat detection and management decision-making.

Daily Reports

- Alarm activations
- Incident summaries
- Operator activity logs
- System health reports

Weekly Reports

- Security trends
- Incident hotspots
- Response times
- Alarm statistics

Monthly Reports

- Executive security dashboard
- Incident trend analysis
- Site risk profiles
- Technology performance reports

Analytics Functions

- AI behavioural analysis
- Motion detection
- Perimeter breach detection
- Object abandonment alerts
- Vehicle detection
- Anomaly detection

11. POPIA COMPLIANCE

All information processed within the Control Room shall comply with the Protection of Personal Information Act (POPIA).

Data Protection Requirements

The Control Room shall ensure:

- Secure storage of all video footage.
- Restricted access to personal information.
- Encryption of transmitted data.
- Auditable access logs.
- Controlled viewing permissions.
- Defined retention periods.
- Secure disposal of records.

Access Control

Only authorized personnel may access:

- CCTV footage
- Incident records
- Access control records
- Analytics reports

Confidentiality

All operators shall sign Confidentiality and Information Security Agreements before receiving system access.

12. SYSTEM SECURITY

The contractor shall maintain:

- Encrypted communication tunnels.
- Network segmentation.
- Secure firewalls.
- System backups.
- Disaster recovery capability.
- Anti-malware protection.
- Cybersecurity monitoring.

---

13. LICENSING AND ACCREDITATION

All software licences, maintenance agreements, subscriptions, and accreditation fees required for the operation of the Control Room shall remain valid throughout the contract period.

The Service Provider shall:

- Maintain all software licences.
- Maintain manufacturer support agreements.
- Maintain cybersecurity subscriptions.
- Maintain analytics platform licences.
- Maintain CCTV management software licences.
- Maintain accreditation requirements.

No additional licensing costs shall be incurred by Eskom during the contract period

14. BUSINESS CONTINUITY

The Control Room shall maintain operational readiness through:

- UPS systems
- Backup generators
- Redundant network paths
- Data backups
- Disaster recovery procedures
- Alternate communication channels

Critical services shall remain operational during power interruptions and system failures.

15. TRAINING REQUIREMENTS

All Control Room personnel shall undergo training in:

- CCTV operations
- Alarm monitoring
- Incident management
- POPIA compliance
- Emergency response
- Eskom security procedures
- Communication protocols
- System operation

Refresher training shall be conducted annually.

16. AUDIT AND COMPLIANCE

Quarterly audits shall be conducted to assess:

- SOP compliance
- Incident response performance
- System availability
- POPIA compliance
- Operator competency
- Contractor performance

Corrective actions shall be implemented for all identified non-conformances.

18. ROLES AND RESPONSIBILITIES

18.1 Control Room Operator

The Control Room Operator is responsible for the continuous monitoring of all integrated security systems and shall:

Surveillance Monitoring

- Monitor CCTV cameras and video wall displays continuously.
- Monitor site-specific high-risk locations and critical infrastructure.
- Identify and verify suspicious activities, intrusions, or security breaches.
- Conduct video verification of alarms and incidents.
- Capture and preserve video evidence when required.

Alarm Monitoring

- Receive, acknowledge, and verify all alarms.
- Classify alarms according to priority levels.
- Escalate alarms in accordance with escalation protocols.
- Coordinate first-line response actions.

Incident Management

- Open incident records immediately upon notification.
- Record all actions taken during incidents.
- Maintain accurate incident logs.
- Update supervisors regarding incident developments.

Communication

- Maintain communication with:
    - Security Officers
    - Armed Response Teams

    - Eskom Security Personnel
    - SAPS
    - Emergency Services
- Ensure all communications are professional and documented.

Reporting

- Complete daily occurrence books and electronic logs.
- Generate incident reports.
- Submit shift reports to the Supervisor.

18.2 Senior Control Room Operator

The Senior Operator shall provide operational leadership during a shift and shall:

- Oversee control room activities.
- Manage operator performance and workload.
- Verify incident classifications.
- Coordinate responses to major incidents.
- Ensure compliance with Eskom policies and procedures.
- Conduct quality assurance on control room records.
- Assist in operator training and mentoring.
- Act as Shift Commander in the absence of the Supervisor.

18.3 Control Room Supervisor

The Control Room Supervisor is responsible for the overall management of each shift.

Operational Management

- Ensure uninterrupted 24-hour control room operations.
- Supervise all operators and support personnel.
- Manage incident escalation and response coordination.
- Ensure all incidents are addressed appropriately.

Compliance Oversight

- Ensure compliance with:
    - Eskom Security Policies
    - POPIA
    - Occupational Health and Safety Requirements
    - Contractor Service Level Agreements

Stakeholder Coordination

- Liaise with:
    - Regional Security Management
    - Security Service Providers
    - Emergency Services
    - Technical Support Teams

Reporting Responsibilities

- Review daily incident reports.
- Verify occurrence book entries.
- Prepare weekly and monthly performance reports.
- Monitor control room KPIs and SLAs.

18.4 Security Risk Manager

The Security Risk Manager shall:

- Provide strategic oversight of the Control Room.
- Approve security procedures and protocols.
- Review incident trends and security risks.
- Approve escalation of major security incidents.
- Coordinate with law enforcement agencies.
- Conduct periodic audits and inspections.
- Monitor contract compliance.

18.5 Technical Support Team

The Technical Support Team shall:

- Maintain all control room systems.
- Maintain communication infrastructure.
- Ensure network availability and cyber security controls.
- Perform software upgrades and patch management.
- Conduct preventative maintenance.
- Maintain backup and disaster recovery systems.
- Ensure all licenses remain current throughout the contract period.

18.6 Security Service Provider

The Security Service Provider shall:

- Ensure 24/7 monitoring capability.
- Provide trained and PSIRA-registered personnel.
- Maintain operational readiness.
- Ensure all incidents are responded to within agreed SLAs.
- Maintain confidentiality of all Eskom data.
- Ensure all integrated technology remains operational.

19. SHIFT HANDOVER PROCEDURES

19.1 Objective

Shift handovers shall ensure continuity of operations, elimination of information gaps, and accountability between outgoing and incoming personnel.

No operator shall leave duty until a formal handover has been completed and accepted.

19.2 Handover Timing

Activity	Duration
Arrival of Incoming Shift	15 Minutes Before Shift Start
Formal Shift Briefing	10 Minutes
System Verification	5 Minutes
Handover Acceptance	5 Minutes

The total handover period shall not be less than 15 minutes.

19.3 Outgoing Shift Responsibilities

Before handover, outgoing personnel shall:

Operations Review

Provide details regarding:

- All incidents attended during the shift.
- Open incidents still under investigation.
- Critical alarms received.
- Escalations made.
- Outstanding actions requiring follow-up.

System Status Review

Confirm operational status of:

- Video Wall

- CCTV Systems
- Access Control Systems
- Alarm Monitoring Systems
- Communication Systems
- Servers and Storage Systems
- UPS and Backup Systems

Documentation Review

Update and complete:

- Electronic Incident Logs
- Occurrence Book
- Alarm Registers
- Visitor Registers
- Maintenance Logs

Evidence Management

Ensure all:

- Screenshots
- Video clips
- Photographs
- Incident records

have been securely stored and referenced.

19.4 Incoming Shift Responsibilities

Incoming personnel shall:

Information Verification

Review:

- Occurrence Book
- Incident Management System
- Alarm History
- Outstanding Incidents
- Daily Notifications

Operational Checks

Verify functionality of:

- Operator Workstations

- Video Displays
- CCTV Feeds
- Alarm Console
- Radios
- Telephones
- Backup Communication Devices

Confirmation

The incoming senior operator shall sign and acknowledge acceptance of the shift.

20. SHIFT HANDOVER CHECKLIST

The following minimum items shall be discussed at every shift change:

Security Incidents

□ New incidents reported

□ Incidents still active

□ Alarm activations

□ Armed response deployments

□ SAPS cases opened

□ Emergency incidents

Operational Issues

□ System faults

□ Communication failures

□ Camera outages

□ Access control faults

□ Network issues

□ Power supply concerns

Intelligence and Threat Information

□ Crime trends

□ Security alerts

□ Protest actions

□ Community disturbances

□ Threat intelligence reports

□ High-risk sites identified

Pending Actions

□ Site inspections pending

□ Maintenance requests pending

□ Management reports outstanding

□ Contractor follow-up actions

□ Outstanding escalations

21. SHIFT HANDOVER REGISTER

Each handover shall be recorded and contain:

- Date
- Shift
- Time
- Name of Outgoing Operator
- Name of Incoming Operator
- Supervisor Name
- Incident Summary
- Outstanding Issues
- System Status
- Signatures

The handover register shall be retained for audit purposes for a minimum period determined by Eskom's records management and POPIA requirements.

22. NON-COMPLIANCE DURING HANDOVER

The following shall constitute non-compliance:

- Failure to conduct a formal handover.
- Leaving a post before relief arrives.
- Failure to report active incidents.
- Failure to disclose system faults.
- Incomplete documentation.
- Failure to update incident records.

Such instances shall be reported immediately to the Control Room Supervisor and Security Risk Manager for corrective action.

Development Team

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

- Musa Mchunu - Security Manager KZNOU
- Jayson Ogle - Officer Area
- Sandise Phili - Assistance Officer