ESKOM DISTRIBUTION

CONTRACTOR'S SECURITY CONTROL ROOM MINIMUM REQUIREMENTS

Tender Compliance, On-Site Evaluation and Operational-Readiness Verification

Document Control

Title	Contractor's Security Control Room Minimum Requirements
Purpose	To prescribe measurable minimum requirements and verification evidence for bidders.
Contractual use	To be incorporated into the RFP, Service Information, technical evaluation criteria and operational-readiness test plan.
Owner	Eskom Distribution Security
Review cycle	As required by contract governance and applicable Eskom standards.

Contents

1. Purpose and status 3
2. Definitions, abbreviations and general obligations 3
3. Mandatory Physical and Facility Requirements 5
4. Personnel and Operating Model 6
5. Technology, Integration and Communications 7
6. Cybersecurity and Protection of Information 9
7. Resilience, Backup Power and Continuity 10
8. Environmental, Welfare and Ergonomic Requirements 11
9. Records, Reporting and Assurance 12
10. Pre-Award and Operational-Readiness Evaluation 12
Annexure A: On-Site Control Room Evaluation Checklist 15
Annexure B: Bid Evidence Submission Schedule 17

Application note

These requirements supplement the applicable Eskom security specifications, contract conditions, Service Level Agreement, Site Technology Schedule, Control Room Interface Schedule and approved technical design. Where a conflict exists, the contract hierarchy shall apply.

1. Purpose and status

1.1 Purpose

The purpose of this document is to define the minimum physical, operational, technological, cybersecurity, information-protection, resilience and personnel requirements for a Contractor-operated Security Control Room supporting Eskom operations.

1.2 Status of requirements

Unless a requirement is expressly designated as desirable, every requirement is mandatory. The bidder shall provide documentary evidence with its tender and shall make the proposed facility, systems, records and personnel available for Eskom verification.

1.3 Inspection rights

Eskom may conduct announced or unannounced inspections before award and throughout the contract. Verification, witnessing or acceptance does not relieve the Contractor of responsibility for compliance, performance, safety, security or continuity of service.

1.4 Misrepresentation

Any material inconsistency between the tender submission and the capability demonstrated during an on-site evaluation may be treated in accordance with the published tender conditions and applicable procurement process.

2. Definitions, abbreviations and general obligations

2.1 Definitions

Definition	Explanation
Alternate Control Room	A secondary facility or approved recovery arrangement capable of assuming the Eskom monitoring service within the recovery period specified in the contract or SLA.
Bidder / Tenderer	A person or legal entity submitting a tender in response to Eskom's invitation and proposing to provide the required services.
Business Continuity	The capability to continue or recover critical control-room services following a disruption, including people, facilities, technology, communications, information and third-party dependencies.
Contractor	The successful tenderer appointed by Eskom to provide the contracted security control-room services.
Control Room	A secure facility from which alarms, CCTV, access-control events, system-health alerts, incidents, dispatch activities, communications and response resources are continuously monitored, coordinated, recorded and reported.

Critical Requirement	A requirement whose failure presents a material risk to security, safety, information protection, resilience or service readiness and which is assessed in accordance with the published tender or go-live criteria.
Dedicated Eskom Desk	A segregated operational position, technology environment and work queue reserved for Eskom operations, with authorised personnel, dedicated displays and controlled access.
Disaster Recovery	The planned restoration of technology, data, communications and supporting infrastructure after a major disruption.
Eskom Information	All data, video, audio, alarms, logs, configurations, reports, credentials, personal information and incident records created, received, processed or retained for the Eskom service.
Incident	An event or condition requiring assessment, recording, escalation, response, investigation or corrective action under the approved Eskom procedures.
Mandatory Requirement	A compulsory requirement that the tenderer or Contractor shall satisfy and evidence at the applicable tender, evaluation, readiness or operational stage.
Multi-Factor Authentication	An authentication method requiring two or more independent verification factors before access is granted.
Non-Conformance	A failure to meet a stated contractual, statutory, technical, security, safety or readiness requirement.
Operational Readiness	The verified state in which the facility, personnel, systems, interfaces, communications, resilience measures, procedures and records are available and capable of supporting service commencement.
Personal Information	Information relating to an identifiable person or juristic person as contemplated in POPIA, including video, access, location and biometric information where applicable.
Returnable	A document, declaration, schedule, certificate, drawing, record or other evidence that the tenderer is required to submit at the stage stated in the tender.
Service	The security control-room activities, deliverables and associated obligations to be provided by the Contractor under the contract.
System-Health Monitoring	Continuous monitoring of the availability, capacity, faults and performance of devices, servers, applications, storage, communications, licences, integrations and backup power.
Verification Evidence	Objective, current and traceable information used by Eskom to confirm compliance, including records, certificates, reports, photographs, configurations, interviews, demonstrations and test results.

2.2 Abbreviations

Abbreviation	Explanation
BCP	Business Continuity Plan
CCTV	Closed-Circuit Television
CV	Curriculum Vitae
DRP	Disaster Recovery Plan
GIS	Geographic Information System
GPS	Global Positioning System
HVAC	Heating, Ventilation and Air Conditioning
ICT	Information and Communication Technology
MFA	Multi-Factor Authentication
POPIA	Protection of Personal Information Act 4 of 2013
RFP	Request for Proposal
SLA	Service Level Agreement
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

2.3 General obligations

The bidder shall identify the physical addresses of the proposed primary and alternate Control Rooms, describe ownership or lawful occupancy, disclose all subcontracted elements and confirm that the facilities will remain available for the contract period. The bidder shall also demonstrate sufficient personnel, workstations, bandwidth, storage, licences, display capacity and supervisory coverage for the proposed Eskom scope without degrading services to Eskom or other clients.

3. Mandatory Physical and Facility Requirements

Requirement	Minimum contractual requirement	Verification evidence
3.1 Permanent facility	The primary Control Room shall be located in a permanent brick-and-mortar building or an equivalent engineered permanent structure. A residential dwelling, tent, temporary site office, unmodified shipping container or mobile unit is not acceptable as the primary facility.	Site inspection; occupancy or lease evidence; floor plan; photographs.
3.2 Location and risk	The facility shall be situated in an area that permits reliable 24/7 access, emergency response and telecommunications. The Contractor shall maintain a documented facility risk assessment addressing crime, fire, flood, civil unrest, environmental and utility risks.	Facility risk assessment; emergency access routes; insurance evidence.
3.3 Perimeter and entry protection	The facility shall have controlled entry, suitable perimeter protection, external lighting and CCTV coverage of entry, exit and vulnerable areas. Doors, windows and service openings shall be secured against unauthorised access.	Physical inspection; CCTV demonstration; maintenance records.
3.4 Restricted access	Access to operational, server, records and communications areas shall be limited to authorised persons through electronic access	Live access demonstration; authorised-user list; access report.

	control, preferably biometric or multi-factor, with unique user identification and auditable access logs.	
3.5 Visitor control	All visitors shall be identified, registered, authorised, issued with temporary identification and escorted in restricted areas. Personal recording devices shall be controlled in accordance with the approved information-protection procedure.	Visitor register; visitor procedure; sample temporary pass.
3.6 Internal segregation	Operational areas, server or communications rooms, records storage, rest areas and public or administrative areas shall be physically segregated. The design shall prevent unauthorised viewing or overhearing of Eskom information.	Floor plan; walk-through; visual and acoustic privacy test.
3.7 Fire and life safety	The building shall have compliant fire detection, suitable extinguishing equipment, emergency exits, evacuation signage, emergency lighting and a documented evacuation plan. Fire systems shall be inspected and maintained.	Certificates; inspection tags; drill records; evacuation plan.
3.8 Dedicated Eskom operations area	A dedicated Eskom monitoring desk or segregated Eskom operational zone shall be provided. The position shall not be shared concurrently with another client and shall have dedicated user profiles, work queues, displays and communications.	Physical inspection; login demonstration; logical segregation test.
3.9 Multi-client separation	Where multiple clients are monitored, the Contractor shall enforce physical, logical and procedural segregation to prevent cross-client data access, screen visibility, audio disclosure, incident misrouting or misuse of credentials.	System roles; segregation configuration; operator demonstration.
3.10 Capacity and scalability	The control room shall have spare workstation, display, network, storage and operator capacity to support incident surges, maintenance, training and reasonable growth within the priced scope.	Capacity statement; utilisation report; expansion plan.

4. Personnel and Operating Model

4.1 Continuous operation

The Control Room shall operate 24 hours per day, seven days per week and every day of the year. No shift, meal break, absenteeism, training activity or handover shall result in an unmanned Eskom monitoring position.

4.2 Staffing model

The Contractor shall submit a staffing model showing posts per shift, relief factor, supervisor coverage, leave and absenteeism provision, peak-load arrangements and escalation support. Staffing shall be sufficient to monitor events and manage simultaneous incidents.

4.3 Supervision

An experienced Control Room supervisor or authorised shift leader shall be available at all times with authority to escalate incidents, deploy response resources and activate contingency arrangements.

4.4 Operator experience

Operators assigned to Eskom shall have demonstrable control room, alarm-monitoring, CCTV and incident-management experience appropriate to the systems and risk profile. The bidder shall provide CVs and verifiable employment or service records for proposed key personnel.

4.5 Registration and screening

All personnel shall hold applicable statutory registrations and role-specific authorisations. The Contractor shall conduct identity, criminal-record, qualification, reference and integrity screening subject to applicable law and Eskom requirements.

4.6 Training

Operators shall be trained and assessed in the integrated monitoring platform, CCTV, alarms, access control, incident classification, dispatch, radio and telephone procedure, escalation, report writing, evidence preservation, POPIA, cybersecurity awareness, emergency response and Eskom-specific procedures.

4.7 Competency management

The Contractor shall maintain a current competency matrix, training records, assessment results, certificates and refresher schedule. Personnel shall not perform specialist functions without current competency.

4.8 Shift control

There shall be documented shift rosters, attendance records, pre-shift briefings, formal handovers, occurrence books or electronic logs, fatigue controls and supervisor sign-off.

4.9 Conduct and confidentiality

Personnel shall sign confidentiality undertakings, comply with clean-desk and acceptable-use requirements, and be prohibited from unauthorised photography, recording, disclosure, copying or removal of Eskom information.

5. Technology, Integration and Communications

5.1 Workstations and displays

Each Eskom operator shall have a dedicated, business-grade workstation with sufficient processing, memory and graphics capability. A minimum dual-monitor arrangement shall be provided per active operator, supplemented by a suitable shared video wall or large-format displays for situational awareness.

5.2 Integrated software

The environment shall integrate, where required by the approved design, CCTV/video management, alarm and intrusion monitoring, access control, incident and case management, dispatch, mapping or GIS, GPS/vehicle tracking, system-health monitoring, reporting and secure communications.

5.3 Interfaces and interoperability

Systems shall use approved, documented and supportable interfaces. The Contractor shall disclose proprietary dependencies, licence restrictions and integration limitations and shall not introduce an undisclosed restriction that prevents Eskom access, migration or authorised future integration.

5.4 Time synchronisation

All critical systems, cameras, alarms, servers, operator workstations, access systems and incident records shall use a common, secure time source so that audit trails and evidence can be correlated.

5.5 Communications

The Control Room shall maintain reliable voice and data communications, including suitable fixed-line, cellular, radio and electronic communication channels. Critical channels shall have alternative or redundant arrangements.

5.6 Recording and retrieval

Where lawful and required, operational calls, radio traffic, alarms, video and incident actions shall be time-stamped, recorded, protected against alteration and retrievable by authorised personnel in accordance with the approved retention schedule.

5.7 System health

The Contractor shall continuously monitor the health and availability of devices, servers, storage, communications links, licences, databases, backup power and integrations. Faults shall generate alerts and unique incident or work-order references.

5.8 Eskom access

Eskom shall receive secure, role-based and auditable access to agreed alarms, video, incidents, reports and system-health data. Access shall not give Eskom visibility of unrelated client information.

6. Cybersecurity and Protection of Information

6.1 Governance

The Contractor shall maintain approved cybersecurity, information-security, privacy, acceptable-use, access-control, incident-response, backup, retention and secure-destruction policies applicable to the Control Room.

6.2 Network segregation

Eskom services shall be logically segregated from public networks, guest networks, unrelated corporate services and other clients through appropriately configured firewalls, network segmentation and access-control rules.

6.3 Identity and access management

Access shall be unique, role based, least privilege and approved. Multi-factor authentication shall be used for privileged or remote access. Shared accounts are prohibited unless technically unavoidable, formally approved and supported by compensating controls and individual accountability.

6.4 Privileged access

Administrator's access shall be restricted, logged, reviewed and used only for authorised activities. Default credentials shall be changed and dormant, transferred or terminated accounts shall be promptly disabled.

6.5 Endpoint and server security

Supported operating systems and applications, malware protection, secure configurations, device control, application control and host firewalls shall be maintained. Unsupported technology requires an approved, time-bound risk treatment.

6.6 Vulnerability and patching

The Contractor shall monitor vendor advisories, assess vulnerabilities, test patches, maintain rollback plans and apply security updates according to approved criticality and change-control requirements.

6.7 Secure connectivity

Remote access and data transmission shall use approved encrypted channels. Remote support shall be authorised, time-bound, monitored and logged.

6.8 Logging and monitoring

Security, authentication, administrative, configuration and data-access events shall be logged, protected and reviewed. Logs shall support investigation and be retained in accordance with the contract and approved retention schedule.

6.9 Incident notification

Actual or suspected cyber incidents, unauthorised access, malware, data loss, credential compromise or material vulnerabilities affecting Eskom shall be contained, preserved and reported through the agreed Eskom escalation process.

6.10 Eskom information

Eskom data, recordings, logs, configurations, reports and incident records shall be used only to provide the Service. The Contractor shall not disclose, monetise, retain, withhold or transfer such information except as authorised by the contract or required by law.

6.11 Privacy and POPIA

Personal information, including access, location, video and biometric information, shall be processed lawfully, for an authorised purpose, with appropriate access, retention, security, breach-management and secure-destruction controls.

6.12 Removable media and printing

Use of USB devices, removable media, local downloads and printing shall be disabled or restricted. Any approved use shall be logged, encrypted where appropriate and subject to secure custody and destruction.

7. Resilience, Backup Power and Continuity

7.1 Power design

Critical systems shall be supported by conditioned utility power, online UPS capacity and an automatic standby generator or equivalent independent supply. The design shall prevent loss of monitoring, recording, communications and incident handling during supply transfer.

7.2 Demonstrated autonomy

The bidder shall state and substantiate the designed UPS runtime and generator autonomy under the actual connected load. Fuel, refuelling, battery replacement, maintenance and testing arrangements shall be documented and demonstrated.

7.3 Telecommunications resilience

Critical connectivity shall use diverse or independent routes or providers where practicable. Automatic or controlled failover shall be tested and evidence retained.

7.4 Redundancy

Critical servers, storage, recording, network components, databases and communications shall have suitable redundancy or documented recovery arrangements aligned to the required availability.

7.5 Backup and restoration

The Contractor shall perform encrypted, monitored backups of configurations, databases, incident records and other required information. Backup success, retention, off-site or segregated storage and restoration testing shall be evidenced.

7.6 Alternate control room

The Contractor shall maintain an alternate facility or other approved recovery arrangement capable of assuming Eskom monitoring within the recovery period stated in the SLA. The arrangement shall include staffing, connectivity, access, systems, data and communications.

7.7 Business continuity

A current Business Continuity Plan and Disaster Recovery Plan shall identify triggers, roles, communications, manual workarounds, alternate facilities, recovery priorities, dependencies and return-to-normal arrangements.

7.8 Exercises

Power-failure, communications-failure, cyber-incident, evacuation, alternate-site activation, backup-restoration and end-to-end recovery exercises shall be conducted at planned intervals and after material changes.

8. Environmental, Welfare and Ergonomic Requirements

8.1 Climate and ventilation

The Control Room and equipment rooms shall have reliable temperature control, ventilation and environmental monitoring suitable for personnel and equipment. Critical cooling shall be maintained during backup-power operation.

8.2 Lighting

Lighting shall support screen-based work without excessive glare, reflection or eye strain. Emergency lighting shall cover operational areas, exits and routes.

8.3 Noise control

The facility shall minimise noise, echo and distraction through layout, acoustic treatment, equipment placement and controlled conversations. Radio and call audio shall remain intelligible without disturbing adjacent operators.

8.4 Furniture

Desks, monitor arms, consoles and chairs shall be robust, adjustable and suitable for continuous 24/7 use. Workstations shall allow safe viewing distances, neutral posture, cable management and unobstructed movement.

8.5 Ablution and hygiene

Clean, functional and adequately maintained ablution facilities shall be available at all times, with suitable provision for the deployed workforce and accessibility where required.

8.6 Welfare

The facility shall provide a separate rest and meal area, potable water, hygienic food-preparation facilities and first-aid equipment. Rest activities shall not occur at monitoring workstations.

8.7 Housekeeping

Operational and equipment areas shall be clean, orderly and free of trip, fire and electrical hazards. Cabling, storage, waste and consumables shall be safely managed.

9. Records, Reporting and Assurance

9.1 Required records

The Contractor shall maintain time-stamped staffing, shift, access, visitor, alarm, incident, dispatch, response, communication, fault, maintenance, system-health, cybersecurity, backup, training and exercise records.

9.2 Retention and availability

Records shall be retained for the period stated in the contract or approved retention schedule, protected against unauthorised change or deletion and made available to Eskom in an agreed open and secure format.

9.3 Daily and monthly reporting

The Contractor shall submit immediate critical notifications, daily exception reports and monthly performance reports covering staffing, availability, incidents, response, faults, changes, cyber events, backup status, non-conformances and corrective actions.

9.4 Audit cooperation

The Contractor shall provide reasonable access to authorised Eskom representatives, auditors and technical specialists and shall support document review, interviews, system demonstrations, sampling and testing.

9.5 Corrective action

Non-conformances shall be recorded with containment, root cause, corrective action, accountable person, due date and closure evidence. Material readiness failures shall be corrected and re-verified before connection or service commencement.

10. Pre-Award and Operational-Readiness Evaluation

The bidder shall allow Eskom to verify tendered capability through document review, facility inspection, personnel interviews, live demonstrations and controlled tests. The evaluation shall be conducted against the published criteria and shall not introduce unpublished functionality requirements.

10.1 Evaluation stages

Stage	Assessment	Scope	Outcome
Stage 1	Tender submission review	Mandatory documents, declarations, facility details and evidence.	Non-submission of designated mandatory evidence may render the tender non-responsive in accordance with the tender rules.
Stage 2	Pre-award on-site evaluation	Physical facility, staffing, integration, cybersecurity, resilience and live demonstrations.	Material failure of a mandatory capability is recorded for evaluation under the published criteria.
Stage 3	Post-award operational readiness	Final Eskom desk, connectivity, configured systems, trained personnel and end-to-end tests.	No Eskom connection or affected service commencement until critical readiness criteria are satisfied.
Stage 4	Ongoing assurance	Announced or unannounced inspections, record sampling and performance verification.	Non-conformance and corrective-action process applies.

10.2 Mandatory live demonstrations

- Controlled entry and production of an access audit report.
- Operator login using a unique role-based account and access to the segregated Eskom environment.
- Receipt of a test alarm, video verification, incident creation, classification, escalation and dispatch.
- Retrieval and export of an authorised recording and associated audit trail.
- Detection of a simulated link or device failure and generation of a system-health alert.
- Transfer to UPS and standby generation without loss of critical monitoring functions.
- Failover of a critical communications or connectivity service.
- Backup restoration of a representative configuration or record.
- Activation of the alternate control room or approved recovery arrangement.
- Provision of secure Eskom authorised access without exposure of other-client information.

10.3 Critical go-live conditions

The following are critical before connection or service commencement:

- secure dedicated Eskom desk;
- trained and authorised operators;
- 24/7 roster and relief;
- access control;
- approved connectivity;
- operational monitoring and incident software;
- communications;
- recording;
- system-health monitoring;
- cybersecurity controls;
- backup power;
- backup and restoration;
- business continuity; and
- successful end-to-end testing.

Annexure A: On-Site Control Room Evaluation Checklist

Evaluator instruction: mark each item Compliant, Partially Compliant, Non-Compliant or Not Applicable. Record objective evidence and reference photographs, reports, extracts or test records. Requirements designated Critical shall be treated in accordance with the published tender and readiness criteria.

Ref	Area	Evaluation criterion	Class	Tender returnable to be submitted	Result	Evidence / observation	Initials
A1	Building	Permanent brick-and-mortar or equivalent permanent engineered structure	**Critical**	Dated photographs, floor plan and declaration confirming the facility type and construction.			
A2	Building	Control room use and occupancy are lawful and sustainable for contract duration	**Mandatory**	Title deed, valid lease or lawful occupancy agreement covering the proposed contract period.			
A3	Physical security	Restricted electronic access with auditable logs	**Critical**	Access-control description, authorised-user list and sample access audit report.			
A4	Physical security	Visitor registration, authorisation and escort controls	**Mandatory**	Visitor-control procedure, sample visitor register and temporary-pass specimen.			
A5	Physical security	CCTV, intrusion alarm, panic alarm and secure key control	**Mandatory**	Security-system layout, equipment schedule, maintenance records and key-control procedure.			
A6	Safety	Fire detection, extinguishers, exits, emergency lighting and evacuation plan	**Critical**	Fire-compliance certificates, current inspection records, evacuation plan and latest drill record.			
A7	Operations	24/7 staffing with no unmanned periods	**Critical**	Staffing model, shift roster, relief-factor calculation and leave/absence coverage plan.			
A8	Operations	Experienced supervisor or shift leader available at all times	**Critical**	Supervisor roster, CVs, qualifications and delegation/escalation matrix.			
A9	People	Valid registrations, screening and role competence	**Critical**	Valid registrations, CVs, screening declaration/results and role-competency evidence.			
A10	People	Training matrix, assessments and refresher records	**Mandatory**	Training matrix, certificates, assessment records and refresher-training schedule.			
A11	Eskom desk	Physically or operationally	**Critical**	Floor plan, desk allocation,			

		dedicated Eskom desk		photographs and signed segregation declaration.			
A12	Segregation	Eskom systems and data segregated from other clients	**Critical**	Logical and physical segregation design, role matrix and data-flow diagram.			
A13	Workstations	Dedicated workstations and minimum dual-monitor arrangement	**Mandatory**	Workstation and monitor schedule, specifications, quantities and dated photographs.			
A14	Displays	Shared display/video-wall capability appropriate to scope	**Mandatory**	Display/video-wall design, specifications, layout and capacity statement.			
A15	Software	Integrated alarm, video, access, incident and dispatch capability	**Critical**	Software functional description, architecture, licences and integration matrix.			
A16	Integration	Documented interfaces, licences and system architecture	**Mandatory**	Interface catalogue, licence schedule, system architecture and dependency statement.			
A17	Communications	Redundant voice and data communication capability	**Critical**	Voice/data design, service-provider details, redundancy diagram and failover method.			
A18	Cybersecurity	Network segmentation and firewall controls	**Critical**	Network diagram, segmentation design, firewall-rule summary and security-control statement.			
A19	Cybersecurity	Unique accounts, least privilege and MFA for privileged or remote access	**Critical**	Identity and access-management policy, role matrix and MFA implementation evidence.			
A20	Cybersecurity	Supported systems, malware control, patch and vulnerability management	**Critical**	Asset/support status, endpoint-security evidence, patch policy and recent vulnerability summary.			
A21	Information	Encryption, logging, retention and controlled export	**Critical**	Information-protection, logging, retention and secure-export procedures.			
A22	Privacy	POPIA-aligned personal-information controls	**Critical**	POPIA compliance statement, privacy policy and personal-information control register.			
A23	Power	UPS supports critical load through generator transfer	**Critical**	UPS specification, connected-load calculation, runtime evidence and test record.			
A24	Power	Automatic standby generator and documented fuel arrangements	**Critical**	Generator specification, load test, maintenance record and fuel/refuelling plan.			

A25	Continuity	Alternate control room or approved recovery arrangement	**Critical**	Alternate-site address, capacity, access, staffing, connectivity and activation plan.			
A26	Continuity	Current BCP/DRP and recent exercise evidence	**Critical**	Current BCP and DRP, latest exercise report and corrective-action status.			
A27	Backups	Successful backup monitoring and restoration test	**Critical**	Backup schedule, latest success report, retention evidence and restoration-test result.			
A28	Environment	Climate control and ventilation operational on backup power	**Mandatory**	HVAC specification, maintenance record and backup-power connection confirmation.			
A29	Environment	Adequate low-glare lighting and emergency lighting	**Mandatory**	Lighting layout, dated photographs, emergency-lighting test and maintenance record.			
A30	Environment	Noise controlled and communications intelligible	**Mandatory**	Acoustic/noise-control description and communication intelligibility test record.			
A31	Ergonomics	24/7-rated desks, chairs, consoles and cable management	**Mandatory**	Furniture schedule, specifications, ergonomic assessment and dated photographs.			
A32	Welfare	Clean ablutions, rest area, water and first-aid provision	**Mandatory**	Facility layout, dated photographs and hygiene/first-aid inspection records.			
A33	Records	Shift, incident, dispatch, fault, access and maintenance records auditable	**Critical**	Sample redacted records, record-retention schedule and audit-trail demonstration description.			
A34	Demonstration	End-to-end alarm, video verification, logging and dispatch test passed	**Critical**	Proposed demonstration script, test plan and available prior test evidence.			
A35	Demonstration	Power failover, communications failover and recovery tests passed	**Critical**	Failover/recovery test plan and latest power, communications and recovery test results.			

Annexure B: Bid Evidence Submission Schedule

Ref	Required evidence	Tenderer submission / returnable	Submission stage	Classification
B1	Control room ownership, lease or lawful occupancy evidence	Certified title deed, signed lease or lawful occupancy agreement valid for the proposed contract term.	Tender	**Mandatory**
B2	Physical address, floor plan and current dated photographs	Signed facility-address declaration, labelled floor plan and dated internal and external photographs.	Tender	**Mandatory**

B3	Facility risk assessment and emergency plan	Current approved facility risk assessment, emergency response plan and evacuation plan.	Tender	**Mandatory**
B4	24/7 staffing model, organogram, rosters and relief calculation	Proposed organogram, posts-per-shift schedule, sample roster, relief-factor calculation and absenteeism coverage plan.	Tender	**Critical**
B5	CVs, registrations, screening process and competency matrix	CVs of key personnel, valid statutory registrations, screening methodology/declaration and completed competency matrix.	Tender	**Critical**
B6	System architecture and integration diagram	Proposed end-to-end system architecture, data-flow diagram, interface schedule and third-party dependency list.	Tender	**Critical**
B7	Hardware, display, software, licence and capacity schedule	Itemised equipment and software schedule showing make/model, quantity, specification, licence basis, utilisation and spare capacity.	Tender	**Mandatory**
B8	Cybersecurity architecture, policies and recent assessment summary	Cybersecurity architecture, applicable policy index, access-control model and recent vulnerability or assurance assessment summary.	Tender / readiness	**Critical**
B9	POPIA and information-protection controls	POPIA compliance statement, privacy and information-protection policies, retention schedule and breach-response procedure.	Tender / readiness	**Critical**
B10	Power single-line diagram, UPS runtime and generator load evidence	Electrical single-line diagram, connected-load calculation, UPS runtime calculation/test and generator capacity/load-test evidence.	Tender / readiness	**Critical**
B11	Connectivity design and redundancy evidence	Primary and backup connectivity design, service-provider details, route diversity, bandwidth and failover-test evidence.	Tender / readiness	**Critical**
B12	BCP, DRP and alternate control room details	Current BCP and DRP plus alternate-site address, capacity, staffing, systems, connectivity and activation arrangements.	Tender / readiness	**Critical**
B13	Backup schedule and restoration-test evidence	Approved backup schedule, latest backup-success report, retention details and completed restoration-test report.	Readiness	**Critical**
B14	Maintenance plans and service records for critical infrastructure	Preventive-maintenance schedules, service-level arrangements and latest service records for power, HVAC, fire, security and ICT systems.	Readiness	**Mandatory**
B15	End-to-end readiness test plan and completed results	Approved readiness test plan, scripts, attendance/witness records, completed results, defects and closure evidence.	Readiness	**Critical**
B16	Non-conformance closure evidence	Non-conformance register showing containment, root cause, corrective action, accountable person, due date and verified closure evidence.	As required	**Mandatory**

Acceptance and Sign-Off

Bidder / Contractor		***Eskom evaluator***
Name		**Name**
Designation	Manager Security	**Designation**
Signature		**Signature**
Date	10 October 2026	**Date**