Installation of a Physical Access Control System

1. Introduction

The SFF Head Office seeks proposals from qualified service providers to supply and install an updated and modernized Physical Access Control System at the SFF Head Office building located at 151 Frans Conradie Drive, Parow. The System should comply with all relevant standards and regulations, including ISO 27001.

Bidders are required to respond to the RFQ with a comprehensive proposal that meets all the specifications outlined in the Scope of Work requirements. Bidders are to also complete and submit the Commercial Bid Analysis that is attached to the tender document, and ensure that all the information requested is included in their submission.

2. Scope of Proposal

The implementation of the system is proposed for the SFF Head Office area, and selected entrance areas to the PetroSA Head Office building in Parow.

The proposal from the selected bidder must include the following requirements:

2.1 PetroSA Head Office_Main Entrances

Boom Gate (SA1)

- LPR technology
- Security Booth
  - Visitor Enrolment
  - Visitor Registration
  - Visitor Induction

Building Entrance 1 (SA2)

- Face Recognition technology
- RFID (Badge/Card, Fob), Fingerprint Biometrics
- Turnstiles (existing)

Garage Gate (SA1)

- LPR technology

Building Entrance 2 (Linked to Parking Garage) (SA2)

- Face Recognition x2 (From Garage & from Doors)
- RFID (Badge/Card, Fob), Fingerprint Biometrics

- Turnstiles (existing)

2.2 SFF Head Office_3rd Floor

- Office Reception (SA3)
- Entry/Exit Doors (x4) (SA3)
- Restricted Access Rooms (x2) (SA5)
- Storerooms (x3) (SA4)
- CEO Suite (x1) (SA3)
- COO Office (x1) (SA3)
- HR Office (x3) (SA3)
- E&P Office (x1) (SA3)
- Exec Office of the CEO (SA3)
- Internal Audit Office (SA3)
- CFO Office (SA3)
- Legal Office (SA3)
- IT Office (SA3)

3. Scope of Work

The SFF Head Office in Parow is relocating from its sub-building to the 3rd floor in the PetroSA Main Building. Occupancy requirements for the office building/floor include ensuring the security of personnel and access control for authorized entry to the SFF office area.

The successful service provider is expected to provide and install a physical access control system that meets the following requirements:

3.1 System Design

The access control system must be capable of using different technologies for ease of access, i.e., LPR, RFID cards, biometrics (fingerprint and face), and Near Field Communication (NFC) technology. Submissions from bidders must detail the proposed approach system design, and how the specified technologies will be incorporated. A description and assurance of the system's compliance with the ISO 27001 Security Standard must also be included in the submission.

The access control system must have the capability to integrate with other systems using open industry standards (or best practice requirements), particularly SAP or similar systems. Proposals from bidders must provide details on the facilitation of seamless data exchange and accurate tracking of employee access and attendance.

Access will be managed centrally at PetroSA Head Office site and must allow granular access rights to various levels of employees, contractors, and visitors. The access control system must allow for real-time monitoring and control of all the access points, using a web-based interface for the management of user access levels, including system configuration and the ability to review audit trails. Bidders are required to submit a comprehensive description of these requirements.

3.2 Access Control Functional Requirements

Bidders must describe the access control methods to be incorporated into the proposed system, including a methodology for ensuring secure and efficient access control (and any other additional features).

The proposal must include a detailed description of the access control system:

- Enrollment process, and methodology for the collection and management of user information and credentials. The system must have its own user management functionality for users registered outside of the ERP and Active Directory parent systems.
- Approach to managing access permission and authorization within the system, and how administrators will grant or revoke access. The system must be able to modify authorizations or access rights or zones for individuals or groups, as and when required.
- Authentication process for validating activated credentials (e.g., ID card, biometrics, pin code, key fob, etc.) for individuals presenting credentials seeking access to premises. Proposals from bidders must describe the validation process for the credentials and how the access control system authenticates all the data.
- Seamless and secure mechanism for granting access once authentication and authorization are completed. Proposals must include a description of how the proposed mechanism will be completed seamlessly and securely.
- Management of monitoring capabilities of the access control system, and how the system will provide accurate and reliable entry logs.
- Storage of access logs for a minimum of 5 years as per internal Policy requirements, and access to logs/reports from other systems and no additional cost. The system must provide the right to access views/tables to consume or create internal reports. Proposals must detail the capability of the control system to manage auditing and reporting, alerting or notification functions, and the generation and storage of access, including internal security regulations and requirements for Data Control and Retention.

4. Access Control Software Requirements

The software for the access control system must meet the following requirements:

4.1 System Management Software

A comprehensive system for managing the entire access control setup, including user interface, functionalities, and efficient and secure remote administration.

Bidders are encouraged to present screenshots of the interface to demonstrate this functionality. The demonstration must also showcase the software's ability to manage user access levels, system configurations, and audit trail review. Additionally, a description of the software's compliance with security standards, including ISO 27001 must be included in the proposals.

4.2 Integration

Ability to seamlessly integrate with other systems (e.g., SAP) required for time and attendance data, and facilitate seamless data exchange.

Proposals must include details on integration capabilities (including integrations with third-party systems), protocols, and methods employed by the software.

4.3 User Management

Allow for granular assignment rights to various levels of employees, contractors, and visitors, based on roles and responsibilities.

Bidders must also include an explanation of user management features (e.g., user enrollment, access permissions), and the ability to adjust as required.

4.4 Real-Time Monitoring

Real-time monitoring and control of all access points, providing administrators with real-time notifications and updates on access events.

A description of the system's ability to ensure a secure and efficient monitoring of access events in real-time must be included in the proposal.

4.5 Security Compliance

Enforce access control and security clearance levels in accordance with relevant standards (as per ISO 27001) and regulations (bidder to specify proposed standards), such as encryption and secure communication protocols, in ensuring that all data within the system is secure.

Proposals must demonstrate the software's capability to meet internal security compliance requirements.

4.6 Reporting and Auditing

Provide robust reporting and auditing features, including generating detailed access logs and related data for a minimum of five (5) years.

Proposals must explain how the software will support the analysis of this data in identifying and responding to security threats. The system must also allow users to define reports as required.

4.7 Emergency Procedures

Capability to manage emergency drills and provide accurate information during emergencies, including facilitating the implementation of emergency lockdown procedures.

Specific features for facilitating emergency response to enhance overall safety and security capabilities must be included in the proposals.

4.8 Scalability

Must be scalable and capable of supporting the growth and expansion of the entities. Proposals must include a description of the management of additional access points, users and system components without compromising performance or security.

Bidders are also encouraged to present examples of the software's scalability in similar deployments.

4.9 Security

Robust security features should be included, that will ensure that all data collected by the system is secure. Bidders must detail information related to the security features, such as encryption and secure communication protocols, that will be incorporated into the proposed solution.

The proposal must include an explanation of the industry-standard encryption methods utilized and confirmation of compliance thereof. A specification of the secure communication protocols supported by their software (e.g., Hypertext Transfer Protocol Secure, or other widely recognized protocols) must also be included in the submission.

Additionally, the submissions must:

a) outline the software's capabilities to ensure integrity and confidentiality of data within the system;
b) address measures for protecting against unauthorized access, data breaches, and any other potential security risk associated with unauthorized data access;

c) relevant certifications, compliance documents, and any supporting evidence to demonstrate the robustness of their security features.

Proposed security features must comply with industry norms, standards and regulations, and provide the necessary assurance that internal data and remain protected and secure throughout the operation of the access control system.

3.10 User Interface

A user-friendly interface that is intuitive and accessible from several devices, including mobile devices, for facilitating easy management and monitoring of access points.

A description of the software's user interface must be included in the proposals. The description must expand on the software's ability to enhance ease of system management, monitoring and administration, and how customization options or user interface personalization features in their software will be addressed.

3.11 Compatibility

Must be compatible with the various hardware components of the access control system, RFID cards, biometrics devices, and NFC devices. Proposals must address any description of specific integration requirements and compatibility testing conducted, in ensuring seamless integration with the proposed hardware components.

All the proposed software components must be reliable, secure, easy to use, and adaptable to the entities' future needs, growths and changes. Proposals must include supporting documentation, case studies, and all suitable references that will aid in demonstrating the reliability, suitability and efficiency of the proposed access control software solution.

5. Access Control Hardware Requirements

Bidders may be required to maintain both existing hardware and supply and install new hardware as part of the access control system implementation. Additionally, Bidders will be required to support and maintain both the new and existing hardware throughout the contract period.

Proposals must include the management of the following hardware components:

5.1 Access Readers

Feature a variety of access reader types, including RFID cards, biometric scanners (fingerprint and face recognition and NFC readers.

An outline of the proposed access reader types and specifications must be included in the submission, and also make an allowance to maintain existing and/or supply new readers to meet the requirements of the access control system.

5.2 Access Cards and Fobs

Compatible with multiple types of physical credentials such as RFID cards and NFC-enabled devices.

In their proposals, Bidders must specify whether they will supply or maintain existing physical credentials and/or supply new ones in line with the requirements of the access control system.

5.3 Door Hardware

Electronic locks, door controllers, door position sensors, and exit devices that are centrally controlled and capable of real-time status reporting.

Proposals must detail the methodology for maintaining or upgrading existing door hardware, and supply and installation of new hardware to meet the requirements of the access control system.

5.4 Turnstiles and Barriers

Description of the proposed barriers for managing and controlling traffic at the main entrances to the building for managing and controlling traffic.

Submissions must include incorporating the use of turnstiles and barriers, and proposals must include maintenance of existing turnstiles and barriers and/or installation of new ones, as required.

5.5 Boom Gates

The system must include boom gates equipped with LPR technology for controlling vehicle access.

The proposed solution must detail whether the existing boom gates will be maintained, upgraded or new ones will be supplied to meet the system specifications.

5.6 Security Booths

Ability to support Security Booths to manage vehicular and user access, including visitor access.

Proposals must outline the system’s support for security booths in controlling vehicle and user access, clearly indicating whether existing security booths will be maintained and/or new one will be supplied.

5.7 Servers and Workstations

A dedicated server for database management and software hosting, including workstations for system administrators.

Proposals must clarify the required specifications for servers and workstations.

5.8 CCTV Equipment

Ability to integrate into existing or future CCTV installations

Proposals must include a methodology for integrating into existing and future installations and details of the hardware requirements for seamless integration.

5.9 Emergency lockdown hardware

Ability to enforce immediate lockdown, utilizing hardware such as emergency push bars, panic buttons, and door lock overrides.

Proposals must include the associated hardware (e.g., emergency push bars, panic buttons, door overrides, etc.) for the system's emergency lockdown capabilities. Clarification on whether existing emergency lockdown hardware will be maintained or upgraded or new hardware will be supplied to meet the system requirements.

5.10 Biometric Devices

Capturing and authentication of biometric data such as fingerprints and facial recognition.

Bidders must describe the proposed biometric devices, and whether existing biometric devices will be maintained and/or new ones supplied as required.

5.11 Integration Hardware

Integration with other software application systems (e.g., SAP) for access control, including application servers and data exchange gateways.

Proposals must outline the required software and hardware for integration and clarify whether existing hardware will be maintained and/or new hardware will be supplied as required.

5.12 Backup Power Supplies

Dedicated backup power supplies for all critical components to ensure uninterrupted operation of the system.

Bidders must detail the proposed backup power supplies, including the type and capacity of backup power supplies. Additionally, a clarification of whether existing supplies will be maintained, or new ones will be supplied as required.

5.13 Networking Equipment

Include requirements for switches, routers, and cabling necessary for connecting and communicating between various components of the physical access control system.

Proposals must also clarify whether existing network equipment will be maintained and/or new equipment will be supplied as required.

Specific Deliverables

- Quotations must include a list of the proposed hardware components, including pricing.
- All hardware components must be robust, reliable and designed for longevity; they must also be scalable and flexible to adapt to SFF's future growth and changes.
- Dependent technologies that will ensure the successful operation of the solution must be clearly specified.
- Bidder must provide comprehensive and detailed information on the access control hardware proposed to be incorporated into the physical access control system, including specifications, technical details and compatibility with required access control methods such as RFID cards, biometric scanners and NFC technology.
- A compulsory site visit is applicable for this tender to confirm the totals as per the table below:

Table 1: Total Devices

Totals		
Device Type	**Biometric**	**RFID**
Main Entrances		
3rd Floor		

6. Security Requirements

Security features such as boom gates with License Plate Recognition (LPR), random search prompts and emergency lockdown procedures must be included in the submissions for the access control system.

Proposals must describe how the proposed system will ensure the security integrity of the access control system, including protection from unauthorized access and data breaches.

6.1 Scalability

The proposed system must be scalable and capable of supporting the growth and expansion of the entities. Proposals must include a description of the management of additional access points, users and system components without compromising performance or security.

Bidders are also encouraged to present examples of the software's scalability in similar deployments.

6.2 Compliance

The access control system must comply with industry norms, standards and regulations, including ISO 27001.

Proposals must provide the necessary assurance that internal data and remain protected and secure throughout the operation of the access control system. Submissions must include relevant certifications, compliance documents, and any supporting evidence to demonstrate the robustness of their security features. Bidder should also explain how the system will ensure ongoing compliance and adapt to any future changes in regulations and standards.

6.3 Training

Submissions must make an allowance to provide training on the operation and maintenance of the access control system.

Proposals must outline the proposed training program, including details on the training curriculum, delivery methods, and all certification programs offered. Submissions must also address the ongoing training and support resources to ensure the internal team is effectively equipped.

6.4 Maintenance

Bidders must make a provision for ongoing maintenance and support for the access control system for the duration of the contract period, and upon. A warranty of 60 (sixty) months for the tender must be provided.

Proposals must detail the program for ongoing maintenance and support services for the access control system, including the duration of the contract period, the frequency of maintenance activities, and response time for attending to system failures and/or issues. Submissions on warranty must include the warranty period and the extent of cover for the software and hardware components.

6.5 Deployment

A description of the deployment plan of the access control system must be provided and should include a deployment approach with clear timelines. The submission must also explain how the deployment plan will ensure minimal downtime and disruptions to business operations during the installation and/or upgrade process.

Bidders must outline the training and support resources they will provide administrators to ensure a smooth transition to the updated and modernized access control system.

- **Seamless integration**

  The system design must integrate smoothly with existing systems and infrastructures (e.g., building management systems, access control points, and surveillance systems)

- **Minimal downtime**

  Disruption to business activities during the installation and upgrade of the access control system must be kept to a minimum and ensure a seamless transition to the updated and modernized access control system.

- **Training and support**

  Administrators must be provided with comprehensive training and support resources, to ensure they are equipped to manage and maintain the access control system effectively.

6.6 Access Control Standards

Access control standards will be developed based on the importance of individual ingress and egress points. The standard will be categorized into the following five levels:

- **Security Access Level 1 (SA1):**
  General Access Points – Allow access to premises only. Access control measures include RFID and/or NFC card access and are typically applied to visitors and contractors (prior

to vetting). Individuals must be escorted or supervised at all times, and random alcohol/drugs testing may be conducted.

- **Security Access Level 2 (SA2):**
  Low-Security Access Points – Less critical access points, with more relaxed security measures. Access control measures include RFID and NFC card access. Typical access to Buildings, Meeting Rooms and Canteens and other general access areas.
- **Security Access Level (SA3):**
  Medium-Security Access Points – Important access points. Access control measures include RFID card access, biometric identification for select employees and contractors. Typical access to Offices.
- **Security Access Level (SA4):**
  Medium-High Security Access Points – Important access points but not to the level of security as Level 5 points. Access control measures include RFID card access, biometric identification for select employees and contractors
- **Security Access Level (SA5):**
  High-Security Access Points - Critical access points that require the highest level of security. They may include sites that contain critical infrastructure. Access control measures include biometric identification, random alcohol/drug testing, and continuous surveillance.

Proposals must outline the approach of Bidders to developing access control standards based on the importance of individual ingress and egress points. Bidders must describe how they will categorize the access control standards into different security levels (SA1 to SA5), according to the level of security required. A clear explanation of how the proposed system will enforce these access control standards must be included in the submissions and the use of appropriate access control methods and measures for each security level.

6.7 Emergency Procedures

Bidders must describe how the proposed system will support emergency procedures, including the ability to manage emergency drills, and provide accurate information during emergencies. Specific features or capabilities of the access control system to facilitate effective emergency response and ensure the safety and security of personnel and facilities must be clearly outlined.

7. Proposal Submission

All proposals must include the following information:

1	Company Information:	A brief history of the company, including experience in the development and implementation of physical access control systems.
2	Project Management:	A description of the project management methodology that will be used to implement the system, including estimated or typical timelines and deliverables.
3	System Architecture:	A detailed description of the proposed system architecture, including hardware and software components, and any third-party integrations.
4	Access Control Methods:	A description of the proposed access control methods, including any additional security features.
5	Compliance:	A detailed description of how the proposed system complies with all relevant standards and regulations, including ISO 27001.
6	Training and Support:	A description of the training and support services that will be provided to the organization's security and technical personnel.
7	Pricing:	A detailed pricing breakdown for all components of the proposed system, including installation, training, and ongoing maintenance. Bidders **must** further complete and attach the Pricing Schedule as per Annexure ii

Annexure iii

Figure 1: 3rd Floor Layout and proposed physical access control locations