CTT25593
TENDER FOR THE PROVISION OF PHYSICAL ACCESS CONTROL FOR PetroSA

PetroSA

SCOPE OF WORK DOCUMENT

Revision	Issue Date	Comments
01	2 May 2023	Draft Initiated
02	26 July 2023	Included CCTV Scope
03	27 July 2023	Scope of Work concluded, ready for publication.

ROLE / DISCIPLINE	INITIAL & SURNAME	SIGNATURE	DATE
ORIGINATOR	MICHAEL ENGELBRECHT	michael.engelbrecht@petrosa.co.za	Digitally signed by michael.engelbrecht@petrosa.co.za Date: 2023.08.18 17:02:06 +02'00'
CHECKED	ESME KLEINHANS	Digitally signed by Esme N Kleinhans DN: cn=Esme N Kleinhans, o=PetroSA, ou=HSEQ-Security, email=esme.kleinhans@petrosa.co.za, c=ZA Date: 2023.08.21 10:18:03 +02'00'	
CHECKED	XOLISWA GORA	xoliswa.gora@petrosa.co.za	Digitally signed by xoliswa.gora@petrosa.co.za DN: ou=RemoteAccess, cn=xoliswa.gora@petrosa.co.za Date: 2023.08.22 11:18:57 +02'00'
REVIEWED	RUBIN BOER		2'/8/2023
APPROVED	JONGKHAYA STUURMAN	jongikhaya.stuurman@petrosa.co.za	Digitally signed by jongikhaya.stuurman@petrosa.co.za DN: ou=RemoteAccess, cn=jongikhaya.stuurman@petrosa.co.za Date: 2023.08.21 11:53:35 +02'00'

1 INTRODUCTION

PetroSA is seeking proposals from qualified service providers for the implementation of an updated and modernised *Physical Access Control System*. The system will be deployed throughout the organisation, which includes multiple sites, some of which are national key points, storage facilities, data centres, and offices. The system should comply with all relevant standards and regulations, including ISO 27001.

2 SCOPE OF WORK

The selected service provider will be required to provide and install a comprehensive *physical access control system* that meets the following requirements:

2.1 SYSTEM DESIGN

The *physical access control system* will be capable of using a variety of technologies including RFID cards, biometrics (fingerprint and face), LPR, and NFC technology to ensure the ease of access. The *physical access control system* will be designed to comply with the ISO27001 security standards.

Bidders are required to provide a detailed proposal outlining their approach to system design and how they will incorporate the specified technologies. Additionally, bidders should explain how their proposed system will ensure compliance with the ISO 27001 security standards.

2.1.1 Integration

The *physical access control system* must have the capability to integrate with other systems to exchange data using open industry-standard (API, OData, etc) which is being used by major ERP such as SAP, or any other systems required for time and attendance data to ensure accurate tracking of employee access and attendance.

Bidders should describe their experience and expertise in integrating access control systems with other systems (using open standards or best practice requirements), particularly SAP or similar systems. They should provide details on how their proposed solution will facilitate seamless data exchange and accurate tracking of employee access and attendance.

2.1.2 Central Management

- Access to the physical premises will be managed centrally at two major sites (Parow Head Office and Mossel Bay Refinery).
- The *physical access control system* will allow for the granular assignment of access rights to various levels of employees, contractors or visitors based on their roles and responsibilities.
- Access rights will be granted and revoked based on the security clearance level, with higher clearance levels requiring additional scrutiny and authorisation.
- The *physical access control system* will be designed to enforce the access control standards and security clearance levels.
- The *physical access control system* should allow for real-time monitoring and control of all access points across all sites.
- The *physical access control system* should use a web-based interface to manage user access levels, system configurations, and review audit trails. This will enable efficient and secure remote administration.

Bidders should provide a comprehensive description of their proposed centralised management capabilities, including how they will manage access rights assignment, security clearance levels, and real-time monitoring and control of access points. Bidders should explain how their web-based interface will facilitate efficient and secure remote administration of the system.

2.2 ACCESS CONTROL FUNCTIONAL REQUIREMENTS

The *physical access control* system should provide a variety of access control methods, including but not limited to RFID cards, biometrics (Fingerprint and/or face recognition) and NFC technology.

Bidders should outline the access control methods (a list of your methods will be appreciated) they plan to incorporate into their proposed system, emphasising how these methods will ensure secure and efficient access control. Bidders should also highlight any additional features or capabilities related to access control they plan to offer.

2.2.1 Layers of Access Control

a) Enrolment

Administrators can enrol users or employees (information from AD/ERP) into the *physical access control system* with their personal information such as name, biometric data (e.g., fingerprints, facial scans), physical credentials (e.g., key fobs, key cards, etc.), or passwords or PIN codes.

Bidders should describe their enrolment process, detailing the methods they will use to collect and manage user information and credentials. They should also explain how their proposed system will ensure the security and accuracy of the enrolment process. Their system should consider the ERP and Active Directory as parent systems and be able to have its own user management functionality in the event a user is to be registered outside of the ERP and AD.

b) **Authorisation**

In this stage, people are given permission to enter the premises, or specific locations on the premises, at specific times. A system administrator gives them access permissions based on a variety of criteria, including whether they are an employee, contractor or visitor, their role, department and more. These permissions (also known as authorisations or access rights or zones) must be able to be modified in the *physical access control system* for individuals or groups of people, as and when needed.

Bidders should outline their approach to managing access permissions and authorisations within the proposed system. They should explain how administrators will be able to grant, adjust, and revoke access rights based on various criteria.

c) **Authentication**

When someone/anyone approaches the premises, they should present a credential, which could be an ID card, biometrics, pin code, smartphone, QR code or key fob, for example. This credential (if activated) allows them to be recognised in the *physical access control* system and, ideally, validated as an authorised user. At this stage, the *physical access control* system also collects data on who is attempting to access the premises.

Bidders should describe the authentication process their system will employ and explain how it will validate the credentials presented by individuals seeking access. Bidders should also address how their proposed system will manage data collection and logging during the authentication process.

d) Access:

If the credential is validated, and the person has the correct access permissions, an electronic output signal is sent to the door, gate, elevator or other point of entry, so to unlock it and allows them to enter. Failed attempts should be recorded.

Bidders should describe their system's mechanism for granting access once authentication and authorisation have been successfully completed. They should explain how their proposed system will ensure a seamless and secure process for unlocking access points.

e) Managing/Monitoring:

System administrators may continually add, remove or alter permissions based on PetroSA's changing needs, and who is expected to be on the premises at which times. These administrators also monitor electronic entry logs to ensure that only authorised users are gaining access to the premises, and to stay abreast of any security threats.

Bidders should outline the management and monitoring capabilities of their proposed system, including how administrators will manage permissions and monitor access events. They should address how their system will provide accurate and reliable entry logs for auditing purposes.

f) Auditing/Reporting:

If there is a security threat (or even a suspicious activity), it is vital that system administrators and security personnel are alerted and are able to closely examine access logs; and if necessary, share data or information with authorities. PetroSA is required to store access logs and other related data for a minimum of 5 years to comply with its security regulations and requirements that it is required to comply, not only with as an oil and gas organisation. Reports should be able to be accessed from other system with no additional cost. PetroSA will have the right to access views/tables to consume or create our own reports.

Bidders should explain how their system will manage auditing, reporting and alerting or notification functions, including the generation and storage of access logs. They should address how their proposed system will ensure compliance with PetroSA's security regulations and requirements regarding data retention.

SCOPE A – ACCESS CONTROL SOFTWARE

3 ACCESS CONTROL SOFTWARE REQUIREMENTS

The physical access control system should incorporate software that meets the following requirements:

3.1 System Management Software

The system should feature comprehensive software for managing the entire access control setup, including system configurations, user access levels, and review of audit trails. This software should provide a web-based interface for efficient and secure remote administration. PetroSA also has perimeter fencing solution and various alarm systems to highlight breaches, the management system should be able to provide a method of highlighting any alarms in various security zone.

Bidders should describe their system management software, including its user interface, functionalities, and how it enables efficient and secure remote administration. Bidders are encouraged to provide screenshots of the interface to demonstrate this functionality. They should emphasise how their software meets the requirements for managing user access levels, system configurations, and reviewing audit trails.

Bidders should also explain how their software complies with PetroSA's security standards, specifically ISO 27001.

3.2 Integration

The access control software should have the ability to seamlessly integrate with other systems such as SAP and any other systems required for time and attendance data. This will ensure accurate tracking of employee access and attendance. The software should also facilitate data exchange with these systems.

Bidders should explain how their access control software integrates with other systems, such as SAP, and how it facilitates seamless data exchange. They should provide details on the integration capabilities, protocols, and methods employed by their software. Bidders should demonstrate their experience and expertise in integrating access control systems with various third-party systems.

3.3 User Management

The software should allow for the granular assignment of access rights to various levels of employees, contractors, or visitors based on their roles and responsibilities. It should also have the capacity to manage access rights based on security clearance levels.

Bidders should outline their software's user management capabilities, specifically how it allows for the granular assignment of access rights based on roles, responsibilities, and security clearance levels. They should describe the user management features, such as user enrolment, access permissions, and the ability to adjust access rights as needed. Bidders should highlight how their software ensures secure and accurate user management processes.

3.4 Real-Time Monitoring

The software should allow for real-time monitoring and control of all access points across all sites, providing administrators with real-time alerts and updates about access events.

Bidders should detail how their access control software enables real-time monitoring and control of all access points across all sites. They should explain the system's ability to provide real-time alerts, notifications, and event monitoring. Bidders should emphasize how their software ensures the security and efficiency of monitoring access events in real-time.

3.5 Security Compliance

The software should enforce access control standards and security clearance levels as per ISO 27001 and any other relevant standards and regulations.

Bidders should explain how their access control software enforces access control standards and ensures compliance with relevant security standards and regulations, including ISO 27001. They should describe the security features, encryption protocols, and data protection mechanisms implemented within their software. Bidders should demonstrate their software's capability to meet PetroSA's security compliance requirements.

3.6 Reporting and Auditing

The software should provide robust reporting and auditing features, including the ability to generate detailed access logs and other related data for a minimum of 5 years. It should also support analysis of this data for identifying and responding to security threats. The user should be able to define reports for their own needs.

Bidders should outline their software's reporting and auditing capabilities. They should explain how their software generates detailed access logs, audit trails, and security-related reports. Bidders should highlight their software's ability to store and retain access logs and related data for a minimum of 5 years, as required by PetroSA's security regulations. They should also emphasise the system's ability to support analysis of access logs and provide insights into security threats. They should demonstrate the ability for users to create their own reports.

3.7 Emergency Procedures

The software should be capable of managing emergency drills and providing accurate information during emergencies. It should also facilitate the implementation of emergency lockdown procedures.

Bidders should describe how their access control software supports emergency procedures. They should explain how the software assists in managing emergency drills and provides accurate information during emergencies. Bidders should address any specific features or functionalities that facilitate emergency response and enhance the overall safety and security of PetroSA's personnel and facilities.

3.8 Scalability

The software should be scalable, capable of supporting the growth and expansion of PetroSA.

Bidders should demonstrate how their access control software is scalable to accommodate PetroSA's growth and expansion. They should explain how their software can manage the addition of new access points, users, and system components without compromising performance or security. Bidders should provide examples or case studies highlighting their software's scalability in similar deployments.

3.9 Security

The software should include robust security features, such as encryption and secure communication protocols, to ensure that all data within the system is secure.

Encryption and protocols to be industry standard compliant.

Bidders are required to provide detailed information related to the security features incorporated into their proposed solution. This should include an explanation of the industry-standard encryption methods utilised. Bidders should also specify the secure communication protocols supported by their software, such as HTTPS (Hypertext Transfer Protocol Secure) or other widely recognised protocols.

Additionally, bidders should outline how their software ensures the integrity and confidentiality of data within the system. They should address measures taken to protect against unauthorised access, data breaches, and any other potential security risks. Bidders are encouraged to provide relevant certifications, compliance documentation, and any other supporting evidence to demonstrate the robustness of their security features.

Please ensure that your proposed security measures align with industry standards and regulations, providing the necessary assurances that PetroSA's data will remain secure and protected throughout the access control system's operation.

3.10 User Interface

The user interface should be user-friendly, intuitive, and accessible from several types of devices, including mobile devices, to facilitate easy management and monitoring of the access control system.

Bidders should describe the user interface of their access control software, emphasising its user-friendliness, intuitiveness, and accessibility from various devices. They should explain how their software's user interface enhances the ease of system management, monitoring, and administration. Bidders should also address any customisation options or user interface personalisation features available in their software.

3.11 Compatibility

The software should be compatible with the various hardware components of the access control system, including RFID cards, biometric devices, NFC devices, and LPR systems.

Bidders should explain how their access control software is compatible with the various hardware components specified in the tender document. They should provide details on the software's compatibility with RFID cards, biometric devices, NFC technology, and LPR systems. Bidders should address any specific integration requirements and compatibility testing conducted to ensure seamless integration with the proposed hardware components.

All software components should be reliable, secure, and designed for ease of use, with the ability to adapt to PetroSA's future needs and changes.

Bidders are encouraged to provide supporting documentation, case studies, and references to demonstrate the effectiveness, reliability, and suitability of their proposed access control software solution.

SCOPE B – ACCESS CONTROL HARDWARE REQUIREMENTS

4 ACCESS CONTROL HARDWARE REQUIREMENTS

The physical access control system should incorporate the management of the following hardware components:

Bidders should carefully review the hardware requirements listed below and provide a comprehensive proposal addressing each component. Bidders may be required to maintain existing hardware if it is already in place, supply new hardware where necessary, install new hardware as part of the system implementation, support both new and existing hardware, and maintain both new and existing hardware throughout the contract period.

4.1 Access Readers

The system should feature a variety of access reader types including RFID card readers, NFC readers, biometric scanners (fingerprint and face recognition), and License Plate Recognition (LPR) readers for vehicle access control.

Bidders should outline their proposed access reader types and specifications, including RFID card readers, NFC readers, biometric scanners (fingerprint and face recognition), and License Plate Recognition (LPR) readers for vehicle access control. Bidders may be required to maintain existing readers, supply new readers, or both, depending on the specific requirements of PetroSA.

4.2 Access Cards and Fobs

The system should be compatible with multiple types of physical credentials such as RFID cards, NFC enabled devices, and key fobs.

Bidders should describe the compatibility of their proposed system with various physical credentials, such as RFID cards, NFC-enabled devices, and key fobs.

Bidders should indicate whether they will maintain existing access cards and fobs, supply new ones, or both, as per PetroSA's needs.

4.3 Door Hardware

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

Bidders should provide details about the electronic locks, door controllers, door position sensors, and exit devices included in their proposed system. They should clarify their approach to maintaining existing door hardware, supplying new hardware, or upgrading existing hardware to meet the system requirements.

4.4 Turnstiles and Barriers

To manage and control pedestrian traffic, the system should incorporate the use of turnstiles and barriers.

Bidders should describe their proposed turnstiles and barriers for managing and controlling pedestrian traffic. They should indicate whether they will maintain existing turnstiles and barriers, supply new ones, or both, based on PetroSA's requirements.

4.5 Boom Gates

For controlling vehicle access, the system should include boom gates equipped with LPR technology.

Bidders should explain their proposed solution for boom gates to be equipped with License Plate Recognition (LPR) technology for controlling vehicle access.

They should clarify whether they will maintain existing boom gates, supply new ones, or upgrade existing boom gates to meet the system specifications.

4.6 Security Booths

For controlling vehicle and user access, the system should include the ability to support Security Booths to manage vehicular and user access, including visitor access.

Bidders should outline their system's support for security booths to manage vehicular and user access, including visitor access. They should indicate whether they will maintain existing security booths, supply new ones, or both, as needed by PetroSA

4.7 Servers and Workstations

The system will require dedicated servers for database management and software hosting, as well as workstations for system administrators.

Bidders should describe the dedicated servers required for database management and software hosting, as well as the workstations for system administrators. They should clarify the required specifications for servers and workstations.

4.8 CCTV Equipment

The system will require integration to existing or future CCTV installations.

Bidders should explain how their proposed system will integrate with existing or future CCTV installations. They should provide details on the necessary hardware required for seamless integration, and clarifying whether they will maintain existing CCTV equipment, supply new equipment, or both, as per PetroSA's needs.

4.9 Emergency Lockdown Hardware

For emergency situations, the system should have the ability to enforce immediate lockdown, utilizing hardware such as emergency push bars, panic buttons, and door lock overrides.

Bidders should outline their system's emergency lockdown capabilities and the associated hardware, such as emergency push bars, panic buttons, and door lock overrides. They should clarify their approach to maintaining existing emergency lockdown hardware, supplying new hardware, or upgrading existing hardware to meet the system requirements.

4.10 Biometric Devices:

Devices for capturing and authenticating biometric data such as fingerprints and facial recognition should be incorporated into the system.

Bidders should describe the biometric devices they propose for capturing and authenticating biometric data, such as fingerprints and facial recognition. They should indicate whether they will maintain existing biometric devices, supply new devices, or both, depending on PetroSA's specific requirements.

4.11 Integration Hardware:

The system should include necessary hardware for integration with other systems such as SAP, including application servers and data exchange gateways.

Bidders should outline the necessary hardware or software required for integrating the system with other systems, such as SAP, including application servers and data exchange gateways. They should clarify whether they will maintain existing integration hardware, supply new hardware, or both, as per PetroSA's requirements.

4.12 Backup Power Supplies:

To ensure uninterrupted operation, the system should have dedicated backup power supplies for all critical components.

Bidders should describe the backup power supplies they propose to ensure uninterrupted operation of the system. They should provide details on the type and capacity of backup power supplies and clarify whether they will maintain existing supplies, supply new ones, or both, as needed by PetroSA.

4.13 Networking Equipment:

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

Bidders should outline the networking equipment, including switches, routers, and cabling necessary for connecting and communicating between various components of the physical access control system. They should clarify whether they will maintain existing networking equipment, supply new equipment, or both, based on PetroSA's requirements.

4.14 Proposal Requirements:

All hardware components should be robust, reliable, and designed for longevity, with the ability to withstand the environmental conditions where they will be deployed. The hardware should also be scalable and flexible to adapt to PetroSA's future growth and changes.

Bidders are requested to clearly indicate any dependant technologies that will be required to ensure the successful operation of the solution.

Bidders should provide detailed information about the access control hardware they propose to incorporate into the physical access control system. This should include specifications, technical details, and compatibility with the required access control methods such as RFID cards, biometric scanners, NFC technology, and LPR readers. Additionally, bidders should explain how their proposed hardware components will meet the specific needs and requirements of PetroSA's access control system.

Include with your proposal, a list of the hardware components that you supply, including pricing.

4.15 Estimated Totals

Estimated Totals		
Device Type	**Biometric**	**RFID**
Total	94	
Parow	76	20
Bloemfontein	4	
Tzaneen	4	
Mossel Bay GTL Refinery	9	268
Mossel Bay (Depot)		12
Heliport (George Airport)	1	8
Saldanha		2
Totals	**188**	**310**

Bidders should confirm totals during their due diligence.

SCOPE C – CCTV REQUIREMENTS

5 CCTV EQUIPMENT REQUIREMENTS

PetroSA is also seeking proposals for the supply, support, and maintenance of an *Integrated Video Surveillance* solution. The solution should meet the specifications outlined in below.

Appendix B contains an exhaustive list of equipment specifications. Please provide pricing on these items as well as an indication of availability. Your proposal should outline your approach to installation, support and maintenance of the end-to-end solution.

Bidders should carefully review the specifications outlined below for the Integrated Video Surveillance solution. Your proposal should address the supply, support, and maintenance aspects of the end-to-end solution. Bidders may be required to maintain existing equipment if it already exists, supply new equipment, install new components, support both new and existing equipment, and maintain both new and existing equipment throughout the contract period.

5.1 Video Analytics System Requirements

The system shall support video encoding with a minimum resolution of 720p or larger, utilising both H.264 and H.265 encoding formats. The compression rate of a single video stream within a 24-hour period, under typical scenarios with varying people and vehicle flows (large, medium, or small), shall be equal to or exceed 60%. The recognition error rate based on compressed video shall not exceed 2%.

Bidders should clearly outline the capabilities of the proposed system. It should support video encoding with resolutions of 720p or higher, utilising H.264 and

H.265 encoding formats. The compression rate of a single video stream within 24 hours should be equal to or exceed 60%, and the recognition error rate based on compressed video should not exceed 2%.

- The system shall support both GPU-based analysis and CPU-based analysis.
- The memory shall be greater than or equal to 512 GB and describe the impact that memory has on the effectiveness of the solution.
- All equipment should be rack mountable, modular in design and utilise redundant and hot-swappable components.
- The system shall support power modules in 1+1 redundancy at least and facilitate independent maintenance of power modules.
- The system shall provide two gigabit ethernet (GE) network ports and two 10 gigabit optical ports. Expansion should be supported.
- A single device shall support at least two types of graphics accelerator cards.
- A single device shall support at most 6 intelligent analysis accelerator cards.
- A single device shall support license plate recognition.
- The system shall support exact and fuzzy search of vehicles by license plate.

5.2 Intelligent Video Integrated Security Management

5.2.1 Unified control:

Integrate video surveillance, access control alarm, AI analysis and other security elements, to build a unified and open intelligent video integrated security platform.

Bidders should outline how their proposed solution offers unified control by integrating video surveillance, access control alarm, AI analysis, and other security elements. The system should be designed to build a unified and open intelligent video integrated security platform.

5.2.2 Open decoupling:

Software and hardware decoupling, algorithm and application decoupling, to build a unified application platform, to convey the value of intelligence for users.

Bidders should describe how their solution allows for software and hardware decoupling, as well as algorithm and application decoupling, to build a unified application platform that can be integrated with the *Physical Access Control System* and convey the value of intelligence to users.

5.2.3 Simple operation:

All service modules are pre-installed, intensively combined, and easy to deploy. The operation is completed based on a unified interface, which is simple and efficient.

Bidders should confirm that all service modules are pre-installed, easy to deploy, and operated based on a unified interface, simplifying the overall operation.

5.2.4 Open SDK

Support for for third-party platforms or mobile application development via an OpenSDK.

Bidders should specify whether their solution provides an open SDK for third-party platforms or mobile application development, facilitating integration and customisation.

5.3 Edge Storage and Analysis Devices

Address the specifications and capabilities of the proposed edge storage and analysis devices based on the following requirements:

- Applicable to small-scale campus scenarios with supports for the connection of up to 64 cameras.
- Support 64-channel network video access (minimum 320 Mbit/s video input)
- At least 4 Tera Operations per Second (TOPS) computing power.
- Support 16 channels of all-channel image-based intelligent analysis.
- Supports advanced video surveillance technology, ensuring that data is still readable and writable in the event of a disk failure.
- Support Video-based target analysis, Behaviour analysis and Video-based vehicle analysis.
- Support for both alarm input and alarm output.

Please ensure that your proposal comprehensively addresses each requirement and outlines your approach to supply, support, and maintenance for the Integrated Video Surveillance solution. Provide details on pricing, equipment availability, installation, and the overall end-to-end solution to meet PetroSA's specific needs, using Appendix B as a guide.

APPLICABLE TO SCOPE A, B AND C

6 SECURITY REQUIREMENTS

The *physical access control* system should include security features such as boom gates with License Plate Recognition (LPR), prompting for random searches, such as alcohol and/or drug testing, and emergency lockdown procedures.

Bidders should outline their approach to security in the physical access control system. This should include the inclusion of security features such as boom gates with License Plate Recognition (LPR), random search prompts (e.g., alcohol and/or drug testing), and emergency lockdown procedures. Bidders should also address how their proposed system will ensure the security and integrity of the access control process, including protection against unauthorised access and data breaches.

6.1 Scalability

The *physical access control* system should be scalable to accommodate PetroSA’s growth and expansion.

Bidders should demonstrate the scalability of their proposed physical access control system. This includes providing information on how their system can accommodate PetroSA's growth and expansion, including the ability to add new access points and users without significant disruptions to the existing system. Bidders should explain how their proposed solution can be easily scaled up to meet future needs and increased requirements.

6.2 Compliance

The *physical access control* system should comply with all relevant standards, regulations and legislations, including ISO 27001.

Bidders should provide evidence of how their proposed physical access control system complies with all relevant standards, regulations, and legislation, including ISO 27001. This should include documentation and certifications demonstrating compliance with industry best practices and security standards. Bidders should also explain how their system will ensure ongoing compliance and adapt to any future changes in regulations or standards.

6.3 Training

The service provider shall provide training to PetroSA's security personnel on the operation and maintenance of the *physical access control* system.

Bidders should outline their training program for PetroSA's security personnel on the operation and maintenance of the physical access control system. This should include details on the training curriculum, delivery methods, and any certification programs offered. Bidders should also address ongoing training and support resources that will be provided to ensure PetroSA's security personnel are equipped to effectively operate and maintain the access control system.

6.4 Maintenance

The service provider shall provide ongoing maintenance and support for the *physical access control* system for the duration of the contract period on award and provide a warranty with its tender for a period of 60 months.

Bidders should provide details on the ongoing maintenance and support services they will offer for the physical access control system. This should include information on the duration of the contract period, the frequency of maintenance activities, and the response time for addressing any system issues or failures. Bidders should also specify the warranty period they will provide with their tender and the extent of the coverage for the hardware and software components of the system.

6.5 Deployment

The new *physical access control system* will be deployed in phases. Primary access points will be secured within one year, while other access points, such as doors and various other access points will be secured within two years.

Bidders should describe their deployment plan for the physical access control system. This should include a phased deployment approach, with clear timelines for securing primary access points within one year and other access points within two years. Bidders should explain how their deployment plan will ensure minimal downtime and disruption to PetroSA's operations during the installation and upgrade process. Additionally, bidders should outline the training and support resources they will provide to PetroSA's administrators to ensure a smooth transition to the updated and modernised physical access control system.

- **Seamless integration**

  The *physical access control* system will be designed to integrate smoothly with existing infrastructure and systems, such as building management systems, access control points, and surveillance systems.
- **Minimal downtime:**
  During the installation and upgrade process, any disruption to operations will be kept to a minimum, ensuring a seamless transition to the updated and modernised *physical access control system*.
- **Training and support**

Comprehensive training and support resources will be provided to Administrators, ensuring they are equipped to manage and maintain the *physical 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 standards will be categorised into five levels:

- ***Security Access Level 1 (SA1) (Green):***

  General Access Points – These access points allow access to premises only. The access control measures for these points will include RFID and/or NFC card access and are typically applied to visitors and contractors (prior to further vetting). Individuals are required to be escorted or supervised at all times, and random alcohol/drug testing may be conducted.

- ***Security Access Level 2 (SA2) (Yellow)***

  Low-Security Access Points - These access points are less critical and will have more relaxed security measures. The access control measures for these points will include RFID and/or NFC card access. Typical access to buildings, Meeting Rooms and Canteens and other general access areas.

- ***Security Access Level 3 (SA3) (Orange)***

  Medium-Security Access Points - These access points are important. The access control measures for these points will include RFID card access, biometric identification for select employees or contractors. Typical Access to Offices.

- ***Security Access Level 4 (SA4) (Purple)***

  Medium-High Security Access Points - These access points are important but do not require the same level of security as Level 5 points. The access control measures for these points will include RFID card access, biometric identification for select employees or contractors.

- ***Security Access Level 5 (SA5) (Red)***

  High-Security Access Points - These are critical access points that require the highest level of security. They may include sites that are designated as national key points or contain critical infrastructure. The access control measures for these points will include biometric identification, random alcohol/drug testing, and continuous surveillance.

  Bidders should outline their approach to developing access control standards based on the importance of individual ingress and egress points. They should describe how they will categorise the access control standards into different security access levels (SA1 to SA5) based on the level of security required. Bidders should also explain how their proposed system will enforce these access control standards, including the use of appropriate access control methods and measures for each security access level.

6.7 Emergency Procedures

The *physical access control system* will be able to manage emergency drills as well as provide accurate information during emergencies.

Bidders should describe how their proposed physical access control system will support emergency procedures. This includes the ability to manage emergency drills and provide accurate information during emergencies. Bidders should outline any specific features or capabilities of their system that will facilitate effective emergency response and ensure the safety and security of PetroSA's personnel and facilities.

7 PROPOSAL SUBMISSION

Tenderers should submit with its Tender, a Proposal that 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 organisation'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 Commercial Bid Analysis to its tender.

Bidders should carefully review the requirements listed in the "Proposal Submission" section of the tender document. They should ensure that their proposal includes all the requested information, such as company information, project management methodology, system architecture, access control methods, compliance details, training and support services, and a comprehensive pricing breakdown. Bidders should complete and attach the Commercial Bid Analysis as specified in the tender document.

8 EVALUATION CRITERIA

Evaluation will be based on the below criteria, including the Questionnaire (included with the Returnable Schedule) as per the Tender on the e-Procurement System:

1	Pre-qualification Criteria:	see Questionnaire (included with the Returnable Schedule) on the e-Procurement System
2	Experience and Qualifications of the service provider:	The service provider's experience and qualifications in the development and implementation of *physical access control systems* – Tenderers must complete and submit the Returnable Schedule as attached on the e-Procurement System – proof to be provided.
3	Technical Solution:	Tenderers must submit their Proposal and the proposed *physical access control* system's technical solution/proposal, which should include its architecture, access control methods, security features and compliance with ISO 27001 – proof to be provided.

4	Project Management:	The service providers' proposed project management methodology, including timelines and deliverables.
5	Training and Support:	The service providers' proposed training and support services.
6	Pricing:	The service providers' proposed pricing for all components of the system, which must include a comprehensive and detailed quotation and analysis of the *physical access control systems* and the various related costs. The Cost to Ownership analysis must be reflected on the Commercial Bid Analysis – see e-Procurement system.

9 PRICING

All pricing of quotations must be quoted in South African Rands and Exclusive of VAT.

Appendix A

Please complete all items indicating compliance with the question by indicating “Y” for Yes or “N” for No. Add comments if required AND indicate a reference to the evidence of such compliance in your Tender.

No	Specific User Requirements	Comply (Y/N)	Comments
01	PSIRA Compliance		
02	Single Card or Identifier to be used for access at all sites		
03	Foe Face Recognition: Turnstiles to be linked to the system and open automatically upon recognizing a person		
04	The system must be able to use facial/biometrics/cards for clocking purposes		
05	The system must integrate with SAP to allow for Time and Attendance for the Short-Term Contractors (STC)		
06	The system must have an ability to integrate actual time with SAP cycles		
07	The system to be able to produce data/report on an individual’s clocking history		
08	The system must be able to automatically calculate and report on the total hours worked for a user		
09	The system must integrate with the Cameras at all egress and exit points		
10	Card drops system to be in place to allow for the dropping of the cards by visitors/contractors		
11	The system to be able to deactivate a card/user automatically when the card/ hours of visit expire		
12	The system must be able to produce a persons’ details with photo and department as a form of identification		
13	The system must be able to allow at least 20 000 people per day (during specific projects)		
14	The system must be able to keep history for 5 years or longer		
15	The system must be able to do zoning		
16	The system must also run parallel with the old system, until old system phased out		
17	The system must have a maintenance plan in place for support purposes – enough spares readily available, e.g., printers, printer cartridges, readers etc.		

18	The system must be user friendly for Operators to be able to use it		
19	The system must be able to show the status of persons with regards to various statuses, such as Security Clearance, Medical Fitness, etc.		
20	The system must be able to remind the user when compliance actions are due		
21	The system must be able to show the status of person’s criminal record/ Security clearance status		
22	The system must be able to show the status of person’s Safety Induction record		
23	The system must be able to indicate a user’s Medical Fitness to work status		
24	The system must be able to lock or refuse entry if a user’s clearances, such as Safety Induction, Medical Fitness Test and a security clearance has expired		
25	Access limitation list to be to deny access to flagged personnel.		
26	The system must be able to provide randomised or organised triggers, such as Alcohol/drug test, hold for inspection etc.		
27	Solution must be able to assist with the generation of random search selection.		
28	System to bring a solution on the Vehicle Access Control management		
29	System to be able to distinguish between current employees / visitors and delivery and service contractors		
30	Work permit system access control to be automated		
31	System to make it possible to allow for filling of information online and placing of a signature (signature pad)		
32	The system to allow for positive identity of asset and owner such as laptops, cell phones		
33	Mobile Device scanners for cards like driver’s license/ ID/ Passport, etc		
34	Access control system to be integrated to the PetroSA website or other mobile access, such as an app, for visitors to fill-in the arrival form and watch the induction video prior to arrival on site		
35	System to maintain history on alarms		
36	The system to be able to alert a controller in a form of an alarm a that there is still people in the building after hours		
37	The system to be able to create alarm as notification for the downtime of other devices		

38	Fire Alarm system to also be linked to the access control system		
39	System to be able to block and report any unauthorised entry on the system by security personnel		
40	System to be able to block and report any unauthorised entry on site		
41	System to pick up duplicate profiles – check first ten digits of ID		
42	Possibility of updating information when it is Exported from SAP.		
43	Ability to print fingerprints after enrolment		
44	Integration with Government/ Municipal systems, like NATIS, Fire, Police, etc.		

APPENDIX B

IP Camera Types

Regarding the camera type, the bidder shall select one of the following types according to the environment and purpose of the camera, after site survey:

- Type 1: 2MP Indoor Dome Camera
- Type 2: 5MP Indoor Dome Camera
- Type 3: 8MP Indoor Dome Camera
- Type 4: 2MP Outdoor Bullet IP Camera
- Type 5: 5MP Outdoor Bullet IP Camera
- Type 6: Outdoor Bullet IP Camera (long lens)
- Type 7: Outdoor High Speed PTZ Dome Camera
- Type 8: 8MP Outdoor AI PTZ Dome Camera
- Type 9: Thermal Bullet camera
- Type 10: Thermal PTZ camera
- Type 11: ANPR Camera

Bidder should propose any additional camera type that they believe should be included in the above list.

Following are examples of typical camera specifications. Bidders are required to indicate the specifications of the cameras proposes, which should be either similar or better.

TYPE 1. Specifications of 2MP Indoor Dome Cameras

No.	Description
1	Image Sensor: 1/2.7" 2-megapixel progressive scan CMOS
2	WDR: 120 dB
3	Maximum Radiation Distance: 30 m
4	Video Encoding Format: H.265/H.264/MJPEG
5	Behaviour Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection
6	Computing power: 1 TOPS
7	Power Supply: 12 V DC, PoE (IEEE 802.3af)
8	Ingress Protection Rating: IP67

TYPE 2. Specifications of 5MP Indoor Dome Cameras

No.	Description
1	Image Sensor: 1/2.7" 5-megapixel progressive scan CMOS
2	WDR: 120 dB
3	Maximum Radiation Distance: 30 m
4	Video Encoding Format: H.265/H.264/MJPEG
5	Behaviour Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection
6	Computing power: 1 TOPS
7	Power Supply: 12 V DC, PoE (IEEE 802.3af)
8	Ingress Protection Rating: IP67

TYPE 3. Specifications of 8MP Indoor Dome Cameras

No.	Description
1	Image Sensor: 1/1.8" 8-megapixel progressive scan CMOS
2	WDR: 120 dB
3	Maximum Radiation Distance: 30 m
4	Video Encoding Format: H.265/H.264/MJPEG
5	Behaviour Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection
6	Computing power: 1 TOPS
7	Power Supply: 12 V DC, PoE (IEEE 802.3af)
8	Ingress Protection Rating: IP67

TYPE 4. Specifications of Outdoor Bullet Camera

No.	Description
1	Image Sensor: 1/2.7" 2-megapixel progressive scan CMOS
2	WDR: 120 dB
3	Maximum Radiation Distance: 50 m
4	Video Encoding Format: H.265/H.264/MJPEG
5	Behavior Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection
6	Computing power: 1 TOPS
7	Power Supply: 12 V DC, PoE (IEEE 802.3af)
8	Ingress Protection Rating: IP67

TYPE 5. Specifications of 5MP Outdoor Bullet Camera

No.	Description
1	Image Sensor: 1/2.7" 5-megapixel progressive scan CMOS
2	WDR: 120 dB
3	Maximum Radiation Distance: 50 m
4	Video Encoding Format: H.265/H.264/MJPEG
5	Behavior Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection

6	Computing power: 1 TOPS
7	Power Supply: 12 V DC, PoE (IEEE 802.3af)
8	Ingress Protection Rating: IP67

TYPE 6. Specifications of Outdoor Bullet Camera (Long Lens)

No.	Description
1	Image Sensor: 1/2.7" 2-megapixel progressive scan CMOS
2	WDR: 120 dB
3	Focal Length: 7-35mm
4	Maximum Radiation Distance: 100 m
5	Video Encoding Format: H.265/H.264/MJPEG
6	Behavior Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection
7	Computing power: 1 TOPS
8	Power Supply: 12 V DC, PoE (IEEE 802.3af)
9	Ingress Protection Rating: IP67
10	Surge Protection Rating: 4kV

TYPE 7. Specifications of Outdoor High Speed PTZ Dome Camera

No.	Description
1	Image Sensor: 1/2.7" 2-megapixel progressive scan CMOS
2	WDR: 120 Db
3	Focal Length: 5-165mm
4	Maximum Radiation Distance: 200 m
5	Zoom: 33x optical zoom
6	Video Encoding Format: H.265/H.264/MJPEG
7	Behaviour Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, and loitering detection
8	Computing power: 1 TOPS
9	Power Supply: 24 V AC, PoE+ (IEEE 802.3at)
10	Surge Protection Rating: 6kV

TYPE 8. Specifications of 8MP Outdoor AI PTZ Dome Camera

No.	Description
1	Image Sensor: 1/1.8" 8-megapixel progressive scan CMOS
2	WDR: 120 DB
3	Focal Length: 6-240mm
4	Maximum Radiation Distance: 250 m
5	Zoom: 40x optical zoom
6	Video Encoding Format: H.265/H.264/MJPEG
7	Behaviour Analysis: Fast movement detection, tripwire crossing detection, intrusion detection, area entry/exit detection, loitering detection and automatic tracking
8	Computing power: 2 TOPS
9	Power Supply: 24 V AC, PoE+ (IEEE 802.3at)

10	Surge Protection Rating: 6kV

TYPE 9. Specifications of Thermal bullet camera

No.	Description
1	400x300 VOx uncooled thermal sensor technology
2	25mm Thermal lens 400*300
3	8mm Visual lens 2MP
4	Uses a 1/2.8 inch CMOS image sensor.
5	Supports fire detection, smoking detection, tripwire, intrusion, call detection, target classification, and alarm linkages.
6	Built-in white light and speaker.
7	View videos on the web, app, PC and more
8	Micro SD memory, IP67, PoE, ePoE.
9	Supports up to 18 color palettes.
10	Warranty Period: 3 years
11	Warranty SLA: 12 calendar days after return the broken equipment to RMA

TYPE 10. Specifications of Thermal PTZ camera

No.	Description
1	400x300 VOx uncooled thermal sensor technology
2	50mm Thermal Lens
3	Athermalized Lens(thermal), Focus-free
4	1/2.8” 2Megapixel progressive scan CMOS
5	Powerful 45X optical zoom 3.95mm~177.7mm
6	Support fire detection & alarm
7	Max 240°/s pan speed, 360° endless pan rotation
8	Up to 300 presets, 5 auto scan, 8 tour, 5 pattern
9	7/2 alarm in/out

TYPE 11. Specifications of ANPR camera

No.	Description
2	3.1 mm to 6 mm LPR
3	2688*1520 maximum resolution
4	1/3" Progressive Scan CMOS
5	PoE support
6	32 Kbps to 16 Mbps video bitrate
7	Up to 300 presets, 5 auto scan, 8 tour, 5 pattern
8	Car (including SUV, MPV, Pickup)/truck/bus/van vehicle type recognition