AIRPORTS COMPANY
SOUTH AFRICA

Request for Proposal for the Supply, Installation and Maintenance of an Intelligent Integrated Security Platform

Annexure A – Scope of Work

Confidential

Glossary and Abbreviations

Item	Description
ACSA	Airports Company South Africa
CCTV	Closed Circuit Television
GUI	Graphical User Interface
IT	Information Technology
IISP	Intelligent Integrated Security Platform
PA	Panic Alarm
PIDS	Perimeter Intrusion Detection System
QMS	Queue Management System
RFI	Request for Information
WPO	Western Precinct Office
AVSEC	Aviation Security
ICAO	International Civil Aviation Organisation

Table 1 Glossary and Abbreviations

Definitions	Description
Cluster	Refers to a grouping of airports. Cluster 1 (OR Tambo International Airport and Bram Fischer International Airport), Cluster 2 (Cape Town International Airport, Upington International Airport, George Airport, and Kimberley Airport) and Cluster 3 (King Shaka International Airport, King Phalo Airport, and Chief Dawid Stuurman International Airport).
Operator	Command centre and Security control room Security Systems user.
Security Command Center	Command centre refers to: a central place for security systems management. It carries out supervisory tasks and integrates all systems from airports and ACSA facilities. This is also a central place for crisis management.
Security Control Room	Airport alarms management centre
Intelligent Integrated Security Platform	Refers to a single platform where all ACSA security systems are integrated and reports alarms, events, audio and data in real-time. It is also where security systems are managed through a single user interface.

Table 2: Glossary Definitions

Confidential

AIRPORTS COMPANY
SOUTH AFRICA

TABLE OF CONTENTS

1. INTRODUCTION **5**

1.1. PURPOSE 5
1.2. OBJECTIVE 5
1.3. BACKGROUND 6

2. SCOPE **7**

2.1. IN SCOPE 7
2.1.1.FUNCTIONAL REQUIREMENTS 7
2.1.2.NON-FUNCTIONAL REQUIREMENTS 10
2.2. OUT OF SCOPE 12

3. FUNCTIONAL / SYSTEMS INTERACTION OVERVIEW **13**

3.1. CONCEPTUAL DESIGNS 13

4. SYSTEM INTERGRATION LIST **18**

4.1. List of existing Systems 18
4.2. List of Future Systems 19

5. SUPPORT AND MAINTENANCE **19**

5.1. SUPPORT AND MAINTENANCE SERVICES 19
5.2. DEFINITION OF INCIDENTS, PRIORITIES AND SLA's 20
5.3. INCIDENT MANAGEMENT RESPONSE AND RESOLUTION TIMES 20
5.4. INCIDENT LOGGING PROCEDURE 21
5.5. IMPLEMENTATION SLAs 21
5.6. BREACH AND PENALTIES 22

6. REPORTING **24**

6.1. WEEKLY AND MONTHLY REPORTS 24

7. MEETINGS **27**

8. DOCUMENTATION **29**

9. SOLUTION GUIDELINES **29**

Confidential

TABLES

Table 1 Glossary and Abbreviations

Table 2: Glossary Definitions

Table 3: Functional Requirements

Table 4: Incident Response and Remediation Time

Table 5: SLA breaches and penalty for incidents

Table 8: Reporting Matrix

Table 9: Meetings Matrix

Confidential

1. INTRODUCTION

1.1. PURPOSE

Airports Company South Africa SOC Ltd hereby invites proposals for the supply, installation, commissioning, testing, maintenance and support of an Intelligent Integrated Security Platform system for the period of 5 years (60 months).

1.2. OBJECTIVE

The objective of this procurement is to obtain a technology solution that must add value to ACSA's existing security services and take into account its existing system architecture. The solution must support the following strategic objectives:

- Improve efficiencies and incident response rates;
- Digitisation and automation of ACSA airports and facilities' security systems;
- Cost optimisation;
- Efficient allocation of people resources;
- Drive higher levels of security;
- Improve the safety and security of people, assets and information;
- Centralise security data and information;
- Reach set security level targets;
- Optimise existing system architecture;
- Increase the threat response rate;
- Improve the quality of security data and information (accuracy, timeliness, completeness and relevance);
- Improve overall awareness of any situation or current status of the airport;
- Improve business continuity;
- Increase the confidence level of employees, at all levels, to respond accurately to potential security breaches;
- Improve management decision making; and
- Design and implement solutions with potential commercial value.

Confidential

1.3. BACKGROUND

Airport security provides an environment wherein passengers, staff, aircraft, and airport property are given assurance and protection from accidental or malicious harm, crime, terrorism and other unlawful acts. Evolution of airport security environments and rapid technological advancement has in recent years highlighted the need for airports around the world to develop and co-ordinate their security systems and functions into well-managed and streamlined operations. Effective airport security management involves far more than having the right security systems in place - it requires systems to be integrated and services to be continually updated and managed from centralised locations.

As noted by the South African Civil Aviation Authority (SACAA), “the primary objective of international civil aviation security is to ensure the protection and safeguarding of passengers, crew, ground personnel, the general public, aircraft and facilities of an airport serving international civil aviation, against acts of unlawful interference perpetrated on the ground or in-flight”. In response to the risk posed by these threats, Airports Company South Africa (ACSA) has deployed various security systems and techniques, such as access control and closed-circuit television, to ensure the safety of its airports. These systems currently operate independently of each other and are not integrated on a single platform. In addition, the lack of integration has resulted in suboptimal utilisation of the existing infrastructure.

Confidential

2. SCOPE

ACSA is looking for a solution that receives logs and events in near real time from, amongst other security systems, Access Control, CCTV (Closed Circuit Television System), and PIDS (Perimeter Intrusion Detection System). This Intelligent Integrated Security Platform should perform event correlation, prioritization, and automated even and incident response. The solution should be managed from a centralized graphical user interface (GUI) with multiple role-based views. The solution should also be able to send out automated notifications for priority events and incidents via email and SMS.

The following sections consist of requirements that are in scope to detect, recover and respond.

2.1. IN SCOPE

2.1.1. FUNCTIONAL REQUIREMENTS

The following are considered an integral part of business needs that are going to be enabled by Intelligent Integrated Security Platform.

ID	FUNCTIONAL REQUIREMENT
BR1	**Provide an Intelligent Integrated Security System Design Architecture**
BR1.1	Delivers integrated intelligent security services
BR1.2	Considers the current environment and leverages existing security systems
BR1.3	Complies to regulatory statues such as POPIA, ICAO, CAA
BR1.4	Conforms to the open standard protocols
BR1.5	Centralise administration and storage of data
BR1.6	Geographical mapping of areas
BR1.7	Provide situational analysis or a heat map of high risk or high activity zones
BR1.8	Automation and digitalisation of standard operating procedures against predetermined policies and business rules. In line with International Civil Aviation Organisation (ICAO), AVSEC standards and guidelines
BR2	**Graphical User Interface (GUI)** a) Operator must be able to read and write to any of the security systems from the integrated module, e.g. acknowledge, reset and escalate alarms through the GUI.

Confidential

	b) The solution GUI should be capable of utilising drawings and maps that are 3D and 2D. The solution should support geographical mapping. c) The GUI should be capable of being driven via a touch screen interface.
BR3	**Cybersecurity** a) The cloud platform should comply and meet ISO/IEC 27001 international standard to manage information security within the platform. b) The Intelligent Integrated Security Platform (IISP) platform must also integrate network monitoring tools or software to detect any abnormalities and intrusions on the security system network.
BR4	**External User Interface** The system must be able to provide different user interface view capabilities. The system should provide configurable user interface views for airports, clusters and command centre levels
BR5	**Operating Environment** a) Distributed Integrated platform: A single integration module should be able to operate all security system data/information that is spread across the airport level, cluster level and command centre level. b) Completely scalable model from user to single site to Enterprise version covering multiples airports control rooms across the airports, cluster and centralised command centre. c) A multi-tiered hierarchy (as a federation system) centralises total control but allows individual sites and clusters to maintain control.
BR6	**Business Continuity and Redundancy** a) Integrating module must have redundancy, and in the event of primary module technical failure, it must failover to a secondary or equivalent module to prevent any disruption of system operation and maintain continuity of service b) All regional airports operating from the cluster shall be equipped with a client station for redundancy in an event network/communication to the main cluster is lost; and c) Scalable redundancy, whereby any workstation/server can be automatically promoted to being the primary host to connect with a single sub-system or multiple systems.
BR7	**Infrastructure Specification** The Service Provider must provide the following infrastructure specifications for their system to function optimally: • Servers (CPU, RAM, HDD); • Storage (any additional storage required); • Network (e.g., ports to be opened, the bandwidth required for the solution to work optimally); and • Database (ACSA database standard is Microsoft SQL and Oracle). • ACSA IT Infrastructure Standards

Confidential

<table>
<tr><td></td><td>

ICT Infrastructure hardware equipment that is provisioned from the appointed Service Provider must ensure that all warranties and maintenance agreements of such hardware equipment should be transferred to ACSA's current maintenance contractor
ICT Infrastructure or hardware provisioned and procured through the main contractor should include a three year onsite replace/fix warranty of:

<table>
<tr><td>Critical Priority (P1)</td><td>• Complete service outage or severe business impact.
• This requires immediate attention.
• Response targets: minutes to 1 hour.</td></tr>
<tr><td>High Priority (P2)</td><td>• Significant degradation or major business impact.
• No reasonable workaround available.
• Significant degradation or major business impact.
• No reasonable workaround available.
• Response targets: 1 to 2 hours.</td></tr>
<tr><td>Medium Priority (P3)</td><td>• Moderate impact affecting some users or functions.
• Workaround may be available.
• Response targets are: 2 to 4 hours.</td></tr>
<tr><td>Low Priority (P4)</td><td>• Minor issues, requests, or non-urgent workloads/services.
• Response target: 4 hours.</td></tr>
</table>
</td></tr>
<tr><td>BR8</td><td>Cloud/Hybrid Computing

The proposed IISP solution should preferably be hosted in the cloud. The solution should support hybrid computing model.
Cloud based solutions must be hosted within South Africa or the European Union jurisdictions.
On premise solutions must be hosted in Tier three data centre within South Africa or the European Union jurisdictions.

</td></tr>
</table>

Table 3: Functional Requirements

Confidential

2.1.2. NON-FUNCTIONAL REQUIREMENTS

The following are non-functional requirements that the IISP system must meet.

ID	NON-FUNCTIONAL REQUIREMENT
BR1	**System Physical Location:** a) The system must be accessible in all 9 airports including the Corporate Office.
BR2	**Solution Performance (speed and accuracy):** a) Immediate response when working on the solution. The system query response time should be responsive near real time. b) The system must be able to handle volumes during peak times. c) The system must be able to cater for bandwidth constraints and geographically dispersed locations. d) The system must support video compression for uploads and downloads
BR3	**System Response** a) All alarms, events, data, audio and video streaming exchange on the integrated module must be in real-time
BR4	**Synchronisation** a) Ability to synchronise completed incidents to the server when offline.
BR5	**Scalability** a) The system must cater for future growth. e.g., adding of new functions and/or users
BR6	**Usability** a) The system must be easy to use with minimal training. b) Ease-of-use requirements must address the factors that constitute capacity of the software; to be understood, learned, and used by its intended users. It must also conform to usability standards for the graphical user interface.

Confidential

BR7	**Reliability & Availability (Days / Hours)** a) The system must be available 24/7. b) The solution must cater for high availability, backups and disaster recovery. c) The system must be able to provide historical data
BR8	**Security** a) The system must align with ACSA Information Security policy (Annexure D). b) The system must support open authentication protocols including Kerberos, Open ID Connect and Oauth. c) The system must ensure that the data is transmitted in a non-readable format (encrypted) and has strong key management. The system must provide encryption capabilities for stored data to ensure that data at rest is protected. d) Ensure that there are SSL certificates signed by the commercial CA (Certificate Authority)
BR9	**User Access Rights** a) The system must allow for users and / role-based permissions to be configured in order to control what system features and data users can access.
BR10	**Repeated authentication failure** a) The solution must notify an administrator, in line with the ASA Cybersecurity policy, if it cannot verify the identity of any user. b) In addition, the system should hide unauthorised functionality to users according to their user profiles.
BR11	**Integrity** a) There must be a single source of truth in terms of data and calculations where applicable. b) The solution must protect its communications from unauthorised intentional corruption during transit, including communications between its users. It must also protect its persistent data from unauthorised intentional corruption.
BR12	**Privacy and data ownership** a) The system must comply with ACSA's Information Security policies, including POPI Act b) All data to remain the property of ACSA and be accessible to ACSA in a format that can be easily utilised.

Confidential

BR13	**Audit Trail** a) There must be an audit trail of who created, updated, closed, and deleted (must be authorised by the super users) the record, include the time and date stamp.
BR14	**Service Access** a) All functions must be accessible via laptops, desktops, tablets, and cellphones. b) Stakeholder management function must be accessible via laptop, desktop, mobile and tablet.
BR10	**Operational** a) Business hours are between 8 am and 7 pm. However, the system availability must be 24/7.
BR11	**Business Continuity** a) The system must have an alternative way to ensure business continuity in cases where there is an unfortunate event of downtime. b) The system must be able to perform business functions during downtime, and the system must be synced with the activities that were taking place during the time the system was down. c) The solutions recovery point and recovery time objectives should comply with the ACSA IT Service Continuity policy which will be provided at contracting stage.
BR12	**Local Support.** First line support for the solution will be done by ACSA. Second line support, by the service provider, must be available in South Africa.
BR13	**Integration:** The system should be able to integrate to the following existing applications in Section 3.1 ***Conceptual design*** of this document**.**

2.2. OUT OF SCOPE

Any requirements that are not explicitly defined in this scope of work.

Confidential

3. FUNCTIONAL / SYSTEMS INTERACTION OVERVIEW

3.1. CONCEPTUAL DESIGNS

OVERVIEW

The diagram below is a Conceptual architecture of an Integrated Intelligent Security Platform (IISP) which provides a high-level view of how the airport's security systems work together as one integrated solution. It shows the key security capabilities, how they interact, and how information flows between systems to support monitoring, incident management, and decision-making. The conceptual design focuses on **business capabilities** and **operational processes** rather than details in the underlying technologies, products, or infrastructure.

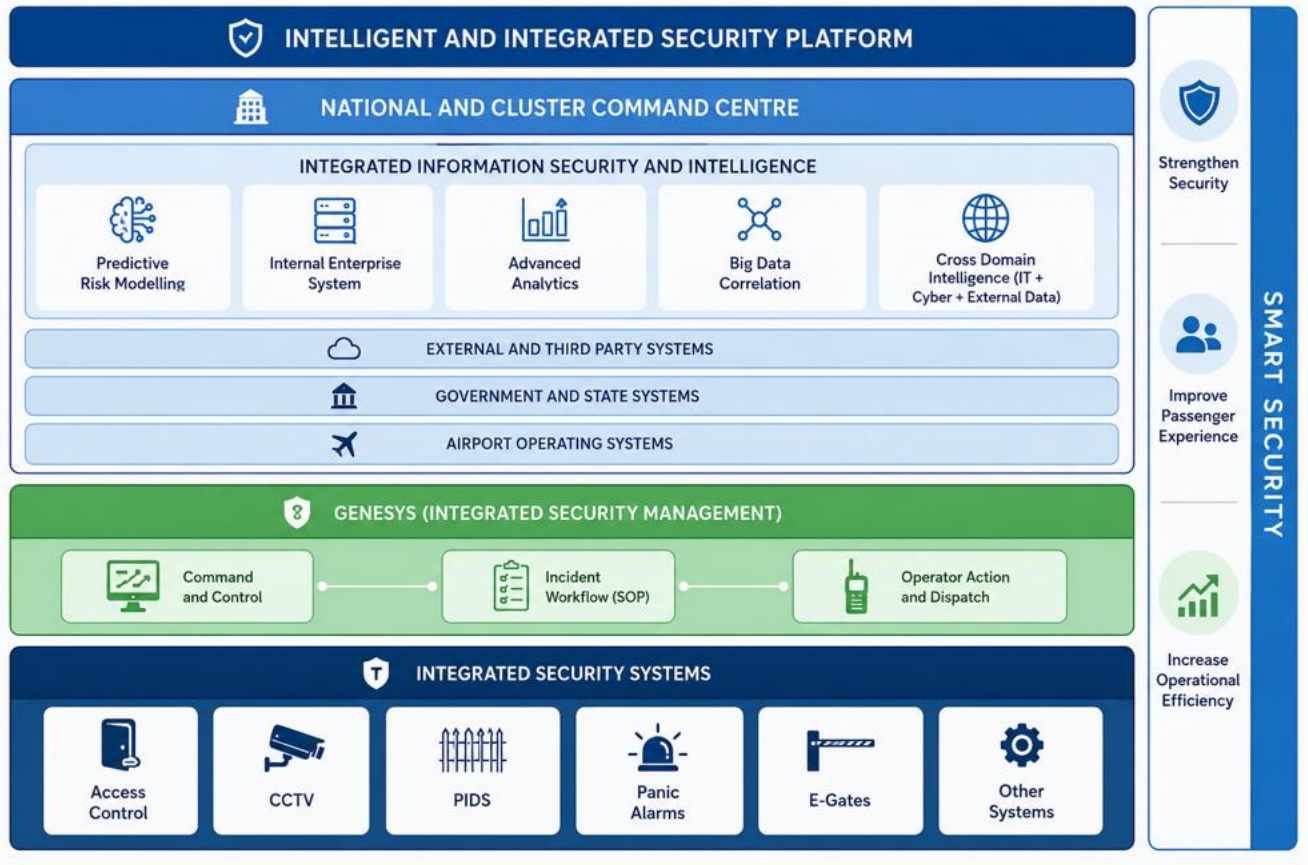


Figure 2: Conceptual architecture of the Integrated Intelligent Security Platform

Confidential

The conceptual solution design is an Intelligent Integrated Security Platform (IISP) for airports that unifies all physical security systems, security operations, and intelligence functions into a single, layered architecture. Its goal is to strengthen security, improve passenger experience, and increase operational efficiency, aligned with global “smart security” concepts.

Device and Sub Layer

At the bottom, the architecture integrates all core security subsystems deployed across the airport: Access Control, CCTV, Perimeter Intrusion Detection Systems (PIDS), Panic Alarms, E-Gates and other specialised systems. These systems generate events, alarms, video streams and access logs.

Integrated Security Systems

Above the devices sits the Integrated Security Systems layer, centred on the Integrated Security Management (a PSIM/ISS-type platform). The platform normalises inputs from all security subsystems and provides a single Command and Control environment, reducing operator workload and improving situational awareness. The platform has three core capabilities are highlighted:

- Command and Control: A single interface to monitor events, visualise locations, view CCTV and control field devices in real time.
- Incident Workflow (SOP): Guided incident management workflows that enforce SOPs from detection through verification, response, escalation and closure, ensuring consistent handling and full audit trails.
- Operator Action and Dispatch: Tools to dispatch patrols or responders, track status, and record all actions, enabling faster, coordinated responses across operations and security teams.

Enterprise and External integration layer

The next layer connects IISP with three key system groups: Airport Operating Systems, Government and State Systems, and External/Third-Party Systems. This allows the platform to exchange incident data, statuses, and risk information with Airport Operations Database (AODB), resource management, airline, and ground-handling systems, as well as police, immigration, and national security agencies.

Through these interfaces, the security platform participates in daily airport operations and regulatory processes, for example: pushing security incidents that may affect operations, consuming intelligence or no-fly lists from authorities, and sharing video or log evidence for investigations.

Intelligence and Analytics Layer

Above operational integration is the Integrated Information Security and Intelligence layer. This layer applies Advanced Analytics, Big Data Correlation, Predictive Risk Modelling, and Cross-Domain Intelligence (IT, cyber, and external data) to all collected information.

It transforms raw events into risk scores, early warning alerts, and trend insights, helping the airport move from reactive to proactive security and operational management. Outputs can include predictive perimeter breach alerts, anomaly detection of access patterns, and cross-correlation of cyber and physical incidents.

National and Strategic Command Layer

On top of the intelligence layer are the National and Cluster Command Centre and the overarching Intelligent and Integrated Security Platform. These tiers provide regional and national views across multiple airports or clusters, consolidating incidents, risks and performance metrics to support centralised decision-making and coordinated crisis management.

This design supports concepts like Aviation Security Management Systems, where security is managed holistically across sites, based on risk and data-driven performance monitoring

Business Outcomes: Smart Security

Running vertically alongside the technical stack, the “Smart Security” column shows that the architecture is designed to deliver three strategic outcomes:

- Strengthen Security: Unified monitoring, analytics and integration with authorities improves threat detection, response times and compliance.
- Improve Passenger Experience: E-gates, automation and better incident management reduce queues and disruptions, aligning with international smart security objectives.
- Increase Operational Efficiency: A single platform, standardised workflows and data-driven planning reduce manual effort, false alarms and duplicated systems, freeing capacity and lowering operating costs.

4. SYSTEM INTERGRATION LIST

4.1. List of existing Systems

Below is a list of existing systems that need to be integrated with the intelligent integrated Security Platform:

4.1.1.1 Access control and permit issuing – Intention is to centralise and use one system across the organisation in future

4.1.1.2 Perimeter Intrusion Detection System – Intention is to centralise and use one system across the organisation in future

4.1.1.3 CCTV

4.1.1.4 Passenger and Baggage Screening Systems

4.1.1.5 Queue Management System

4.1.1.6 Terrestrial Trunked Radio Communication (TETRA)

4.1.1.7 Panic and Fire Alarms

4.1.1.8 Emergency and Fire Doors

Confidential

4.1.1.9 Aircraft Gates and Emergency Gates

4.1.1.10 Patrol Badging System

4.1.1.11 Key Control System

4.1.1.12 Building Management System

4.1.1.13 Airport Management System

4.1.1.14 Smart Security Lanes

4.2. List of Future Systems

Below is a list of possible future systems that will be integrated with the intelligent integrated Security Platform:

4.2.1 Background Check System

4.2.2 Security Incidents Reporting System

4.2.3 Vehicle Intrusion Detection System

4.2.4 Biometrics (e.g. Facial & Finger)

4.2.5 Behaviour Detection System

4.2.6 Remote Piloted Aircraft System

4.2.7 Vehicle / Trucks / Containers X-ray

4.2.8 Watch list of wanted persons

4.2.9 Fleet Tracking System

4.2.10 Case Management

5. SUPPORT AND MAINTENANCE

This section describes what Support and Maintenance entail in general and further describes what maintenance entails for ACSA.

5.1. ACSA requires the Support Services from a Service Provider as described below:

5.1.1. Day to day support activities performed to remediate/report on security incidents, alerts and threat logs generated by the system's internal monitoring;

Confidential

5.1.2. The Service Provider will be required to respond to and remediate all incidents in line with ACSA vulnerability management process. All security incidents will be logged on the IT service desk systems; and

5.1.3. The response and remediation times depicted below must be adhered to. This will form part of the SLA's that will be agreed to between the Service Provider and ACSA.

5.2. DEFINITION OF INCIDENTS, PRIORITIES AND SLA's

Priority 1: Total system failure

Priority 2: Partial system failure with minimum monitoring functionality

Priority 3: Non-critical fault/failure logged at night or over the weekend. It has no impact on the operations of the airport

Priority 4: Minor incidents or move/change or installation of new item

5.3. INCIDENT MANAGEMENT RESPONSE AND RESOLUTION TIMES

Incident management response and remediation times for (Office Hours, After Hours, Weekends and Public Holidays) ***** The service provider will be required to provide support and maintenance on a 24/7/365 basis**			
	Response	**Restoration**	**Update Feedback**
P1	15min	1hrs	Every 30min
P2	30min	4hrs	Every 1hr
P3	2hrs	8hrs	Every 2hrs
P4	4hours	24hrs	Every 8hrs

Table 4: Incident Response and Remediation Time

Confidential

5.4. INCIDENT LOGGING PROCEDURE

ACSA requires the Service Provider to adhere to the following incident logging procedure:

5.4.1. As per the ACSA incident management Procedure (which will be shared with the winning bidder) All security incidents must be logged with ACSA service desk via email, telephone or on the self- service web portal. The incident status must be updated regularly depending on the priority of the incidents until resolution;

5.4.2. All security incidents must be updated with a detailed resolution before closure. The Service Provider must notify the service desk immediately on resolution of the incident.

5.5. IMPLEMENTATION SLAs

5.5.1. The implementation schedule (dates, milestones, success criteria etc.) will be defined in the project kick off meeting. Should such schedule not be agreed to, it is stated that there is no consensus between the parties, and this affects the validity of the contract.

5.5.2. The approved minutes of the kick-off meeting will serve as the agreement by the parties of the service level and penalties.

5.5.3. The approved minutes from the kick-off meeting shall be regarded as an Appendix and form part of this agreement

5.5.4. Where the Service Provider does not meet the implementation dates as documented and agreed by both parties in the kick-off meeting, unless clearly and timeously communicated in writing and the schedule re-baselined by the ACSA project manager, ACSA will notify the Service Provider of breach of service.

5.5.5. The service provider is expected to deliver this project in line with the agreed timelines, milestones and conditions.

5.5.6. The Supplier must propose how to best group features and provide incremental solution design, development, testing and release plan.

5.5.7. For each release that misses the scheduled release date, and or is above System Integration Testing (SIT) to Unit Acceptance Testing (UAT) defect leakage tolerance, ACSA will withhold 10% of the implementation fee per such release. Defect leakage from SIT to UAT must be less than 10% tolerance limit.

5.5.8. The solution must be in early life support for a minimum of four (4) months.

Confidential

5.6. BREACH AND PENALTIES

As detailed in the next sections, the following penalties shall apply in the event of a breach of service levels as agreed. The service provider shall restore the solution that is in scope within times specified in the service level agreement; the following project and operational-based penalties shall apply for failing to deliver the expected milestone or restore the services within agreed timelines:

SLA BREACH	PENALTY
Project SLA Breach & Penalties	
If the project milestone or release misses the scheduled release date and or is above SIT to UAT defect leakage tolerance	10% of the implementation fee per such release will be withheld.
Operational SLA Breach & Penalties	
P1 Incidents are resolved after SLA time lapsed, for two consecutive times in one month across any of the sites in scope	20% of the monthly fee will be deducted per invoice and up to 60% in one contractual year. After that, termination procedures will be implemented.
P2 to P4 Incidents are resolved after SLA time lapsed for three consecutive times in one month across any of the sites in scope	30% of the monthly fee will be deducted and up to 60% in one contractual year. After that, termination procedures will be implemented.
If a Service Provider misses Incident Management SLAs in any three consecutive months across any sites in scope	50% of the monthly fee will be deducted.
If a Service Provider misses Incident Management SLA's consecutive in any 4 months across all site's ins cope – will be deemed as a material breach, and the contract will be referred for performance management and/or termination procedures	50% of the monthly fee will be deducted.

Confidential

Table 5: SLA breaches and penalty for incidents

Failure to perform maintenance and/or services in accordance with the scheduled dates or Priority list and SLA agreements shall result in the following penalties:

Maintenance	Penalty
Maintenance not done or proof of carrying maintenance out not submitted.	No payment of invoice.

Table 6: Failure to provide maintenance

Confidential

6. REPORTING

(a) As part of ongoing performance management, ACSA requires that the Service Provider provides the following reports as contained in the table below. These reports will be presented to ACSA on demand and during implementation and ongoing support of the services.

(b) ACSA reserves a right to change a list of reports as requested and will review these on a regular basis, and such changes should not attract additional costs.

(c) The project meetings will be held weekly, and/or on-demand for the duration of the contract and arranged by the ACSA Information and Enterprise Security teams to discuss the following, but not limited to:

6.1. WEEKLY AND MONTHLY REPORTS

#	Report Name	Frequency	Content and Format	Submitted to
1	Service Request Status (not incidents)	Every day of the week and a consolidated version for all 4 weeks on the last day of the month	Status of new enhancements, fixes, requests	Airport System and Enterprise Security Team

Confidential

2	Weekly Service Review Reports for open, closed incidents, the status of each incident in terms of SLA.	Every day of the week and a consolidated version for all 4 weeks on the last day of the month	Open and closed incidents. Status of each incident in terms of SLA. Reason for SLA breaches, if any and measures that will be put in place to avoid a breach.	Airport System and Enterprise Security Team

	Report Name	**Frequency**	**Content and Format**	**Submitted to**
3	Maintenance reports: report against the maintenance schedule. This will include issues picked up during maintenance.	Every day of the week and a consolidated version for all 4 weeks on the last day of the month	Modules worked on. Issues discovered per module and how they were resolved. Details on any general maintenance work carried out.	Airport System and Enterprise Security Team
4	Monthly Systems Availability Report against the ACSA required target of 99.9 % uptime.	Last day of the month	System availability System downtime	Airport System and Enterprise Security Team

Confidential

5	Preventative work done.	Monthly	Report on various preventative work performed	Airport System and Enterprise Security Team
6	Issues for ACSA's attention.	As and when they occur	Any relevant issues that need to be brought to ACSA's attention by the Service Provider.	Airport System and Enterprise Security Team
7	Ad-hoc	As and when required	Ad-hoc, depending on the request at hand.	Airport System and Enterprise Security Team

Table 6: Reporting Matrix

Confidential

7. MEETINGS

As part of ongoing performance management and project delivery, ACSA requires that the Service Provider attend monthly and weekly meetings.

Frequency	Meeting Name	Standing Agenda	Participants and Role	Prior documents to be submitted by the Service Provider	Documents to be produced after meeting
Monthly	Project Board Meeting	Discuss all aspects of Monthly reports Discuss Project Costs, Timeline, Risks, Issues, Resources, etc. Discuss all deliverables produced to trace successful delivery on Business Requirements.	IT PMO, Service Provider's Service Delivery Manager, ACSA contract owner, ACSA Technical Lead, Project Sponsor, Other Stakeholders per Invitation	Project Board Pack including Planned Presentation. Previous meeting action items Monthly Reports.	Attendance Register Meeting action items

Confidential

Weekly	Progress Meeting	Progress Reporting, Performance Management, Security Posture, Security Incidents/Threats Reporting, Exception Reports, Risk Register, Areas of Focus, discuss high-level service deliverables/milestones, Timelines and delivery, Environment Risks / Issues / Assumptions, Contractual/Financial and Governance, General and all other requirements related to the services. Internal and External Audits of the Services in Scope.	Service Provider's Service Delivery Manager, Technical Resources and ACSA Security team	Minutes of Previous Meeting. Updated Risk and Issue Log.	Attendance Register. Meeting action items Acceptance of deliverables.
Ad-hoc	Ad-hoc	Ad-hoc	Service provider & other relevant Stakeholders as and when required	Ad-hoc	As agreed by all parties
Monthly	Operational Meetings	Review system operations, vendor performance	Service provider & IT Operations Department	Operational reports	Minutes, attendance register.

Table 7: Meetings Matrix

Confidential

8. DOCUMENTATION

The following project-related documentation must be produced by the Service Provider during the implementation of the project:

- Project Management deliverables as per ACSA standards
- Architectural Design
- Functional Specification
- Technical Specification
- Interface Control Document
- Quality Assurance Specific Documentation (Test plan, Test cases, Test results for different types of solution testing (unit, functional, performance, stress, vulnerability, List of Defects)
- Operational Manuals
- Training Manuals

9. SOLUTION GUIDELINES

- The solution must provide the functions and services required to support the business capability.
- There should be a single application to support a given business capability, i.e., the solution must not re- implement a capability already available in the portfolio unless it is replacing the current one.
- The solution must be as secure as business requirements dictate.
- The solution must meet legal and conformance requirements, including those for privacy.
- The solution must provide adequate performance and responsiveness.
- The solution must be able to scale, without redevelopment, for anticipated increase in volumes for the next five years.
- The solution must be reliable and easily recoverable.
- The solution must validate input data and maintain the integrity of any data added, updated or exported.
- The solution must provide APIs which allow services to be accessed via an interface conforming to industry standards adopted by ACSA, e.g., Web Service (REST, SOAP).
- The solution must avoid “hard coding” of value, i.e., any variables which are likely to change must be externalised to the database or parameter/rule files
- The solution must capture errors and report them in a meaningful and persistent way
- The solution end-user interfaces must be intuitive and standards-based to facilitate ease of adoption and reliable usage as well as reduced training requirements.
- The solution must adhere to ACSA’s Cybersecurity policies and procedures including the patch management policy
- The solution must be documented to a standard that facilitates:
  - Ease of installation and configuration.
  - Ease of operation by end-users.
  - Easy problem determination and resolution.
  - Impact analysis for change requests.
  - Ease of adaptation when required; and
  - The solution must not expose ACSA to undue risk.