An Integrated Cloud Email Security Solution

Annexure A – Scope of Work

Glossary and Abbreviations

Item	Description
ACSA	Airports Company South Africa
IS	Information Security
ISM	Information Security Management
IP	Internet Protocol
TLS	Transport Layer Security
DLP	Data Leakage Protection
DMARC	Domain-based Message Authentication, Reporting & Conformance
SPF	Sender Policy Framework
DKIM	Domain Keys Identified Mail
ICES	Integrated Cloud Email Security
SoW	Scope of Work
IOC	Indicator of Compromise
URL	Uniform Resource Locator

Table 1 Glossary and Abbreviations

TABLE OF CONTENTS

TABLES

1 INTRODUCTION

1.1 PURPOSE

Airports Company South Africa SOC Ltd hereby invites proposals for the provision of an Integrated Cloud Email Security Solution for the period of 3 years (36 months).

1.2 OBJECTIVE

The aim of this RFP is to obtain a proposal from Bidders, in respect of the relevant scope of services, and to evaluate these in order to appoint a Service Provider for the provision of an Integrated Cloud Email Security Solution for a period of thirty-six (36) months at ACSA.

The service provider will be required to fulfil the requirements set out in this RFP. The duration of this contract is anticipated to be for a period of thirty-six (36) months. Upon appointment of the Service Provider, a professional services contract shall be concluded with the Service Provider. ACSA may at any time terminate the contract or postpone or delay all or any part of the contract upon written notice to the selected Bidder in line with the prescribed process.

The successful service provider is to provide An Integrated Cloud Email Security Solution which complements the existing ACSA investment in M365 Email security solutions. Through integrating ACSA's existing M365 Email security solution and leveraging improved and innovative Integrated Cloud Email Security components, ACSA can ensure an increased cyber and information security maturity. In doing this, ensuring that ACSA business systems are kept operational and email communication is securely enabled and efficient in order to achieve good customer service, value for money and improved Airport Service Quality (ASQ) ratings.

1.3 BACKGROUND

ACSA is a critical organ of the state, one that interconnects the country with the international economy, operating in an industry that has major appetite for the use of technology not only for profitability but also for providing safety to all stakeholders. In order to pursue its mandate, ACSA has been leveraging technology, digitizing its business operations and bolstering its technology security as our threat landscape and its complexity increases.

The continued use of legacy systems presents a major security risk and requires and innovative approach that not only focuses on the traditional Integrated Cloud Email Security approach, but on long term solutions to replace end of life and unsupported software and technologies. Solutions centered around principles of application rationalization, fit for purpose, ease of use and maximizing business value. ACSA would like to enable an Integrated Cloud Email Security capability that integrates with ACSA's existing exchange online hybrid architecture, while embedding a culture of risk reduction and management.

To enable the achievement of the organization’s digitization journey one which is Secure, Compliant, and Resilient, ACSA requires An Integrated Cloud Email Security Solution to assist them in enabling their Email security capability with an innovate and secure capability. While leveraging their existing technology and Digital Workforce Modernization security solutions. The continuing pandemic effects are being felt in terms of constraints in people and process enablement, whether technology solutions are in place or not fully leveraged.

2 SCOPE

The following sections consist of requirements that are in the scope of provisioning an Integrated Cloud Email Security Solution for ACSA to seamlessly integrate with existing M365 Email Security capabilities.

2.1 IN SCOPE

The scope of the work includes, but not limited to the following key components, required to implement an Integrated Cloud Email Security Solution

REQUIREMENT
Email Security Capabilities • Provide comprehensive email security to protect against primary threat vectors, including: o Business Email Compromise (BEC) o Ransomware o Phishing attacks • High profile user (Executive management and Special classified users) monitoring and protection • Ensure compliance with POPIA by safeguarding personal information processed through email systems and preventing unauthorized access, loss, or misuse of such data • Include automated threat detection and response capabilities to mitigate risks in real time.
Advanced Threat Protection • Implementation of artificial intelligence and machine learning capabilities for detecting sophisticated impersonation attacks. • Support for all standard web browsers and device types.

- Compliance with POPIA to ensure that personal information accessed via email or web-based threats is adequately protected.

DMARC management

- Implement and maintain DMARC protocol to authenticate email senders and protect against phishing and spoofing.
- Ensure integration with existing SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) protocols.
- Provide reporting mechanisms for email validation and disposition.

Protection Against Malicious Attachments

- Provide ACSA with a dedicated capability to enable Attachment-type blocking, Encrypted file blocking (Microsoft Office and Adobe PDF files), quarantining, anti-virus, archive unpacking, detection notices, Email Threat intelligence sharing, Attachment sandboxing and other advanced capabilities to ensure that malware propagation through email attachment exploitation is prevented.

Protection Against Malicious Links

- Provide ACSA with an Integrated Cloud Email Security Solution that will assist with spear-phishing detection, Behaviour-based phishing link detection, bolstering URL reputation in attachments, detection of URL look-alike, scanning of shortened URL’s, Vendor URL IOC’s, URL disarm, URL rewriting and URL redirection capabilities.

Protection Against Impersonation

- Provide ACSA with an Integrated Cloud Email Security Solution that will assist with Reputational spam blocking, Content-based spam blocking, Anomaly detection (volumetric), Sender domain reputation, Own-domain spoof detection (inbound), Authenticated email (DMARC – inbound), Granular DMARC policies, Originating IP address analysis, Anomaly-based impersonation detection (across identity, connection, content and context), Smart tag control for email replies and forwards, protection against account takeover and business email compromise attacks and other impersonation protection capabilities.

Management, Operations and Reporting

- Ensure that the ACSA is enabled with Role-based administration, Role-based graphical user interface (GUI), MFA admin login, Quarantine management, Customization of messages, Alerting, Troubleshooting support, Basic email search, Policy propagation latency, Reporting on clicked links, Detailed sandbox reporting, Log data retention, Log data export, Block lists and allow lists, Availability SLA, DMARC configuration support,

IOC export and sharing, Quarantine notification frequency, Granular scanning policies, Privacy-enabled reporting, Strategic threat intelligence reporting and other Operations and reporting capabilities.
Deployment and Integration • Ensure that ACSA is enabled with an inbound gateway, an outbound gateway, Privacy and data residency, Cross-customer threat intelligence sharing, API integration, SIEM integration, Identity provider integration, Cloud access security broker (CASB) integration, Ticketing system integration, Endpoint protection platform (EPP)/endpoint detection and response (EDR) integration and other integration and deployment and support. ACSA also requires ICES and DMARC implementation services.
Governance Alignment • Ensure adherence to ACSA Enterprise, Cyber and Information Security governance, policies, standards and guidelines
Continuous Improvement • Advise and recommend improvements to the Integrated Cloud Email Security efforts within ACSA, whether related to strategy, framework, policy or any other improvement consideration.

Table 2: Functional Requirements

2.2 OUT OF SCOPE

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

Costing for any M365 related Email security components unless it relates to how the integration will be performed into these components, specifically where partner API's for email security functionality that satisfies the business requirements above is required.

3 SUPPORT AND MAINTENANCE

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

ACSA requires an Integrated Cloud Email Security Solution from a Service Provider as described below:

3.1.1 Day to day support activities to ensure that any issues with the software, operations, governance activities or any other factor related to its Integrated Cloud Email Security operational efficiency to achieve required business requirements

3.1.2 The Service Provider will be required to respond to and remediate all issues related to the Integrated Cloud Email Security solution and its functioning.

3.1.3 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.

3.2 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

3.3 INCIDENT MANAGEMENT RESPONSE AND RESOLUTION TIMES

Incident management response and remediation times for (Office Hours, After Hours, Weekends and Public Holidays)			
	Response	**Restoration**	**Update Feedback**
P1	15min	2hrs	30min
P2	30min	4hrs	1hr
P3	2hrs	8hrs	2hrs
P4	4hours	24hrs	8hrs

Table 3: Incident Response and Remediation Time

3.4 INCIDENT LOGGING PROCEDURE

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

3.4.1 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 is met;

3.4.2 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.

3.5 BREACH AND PENALTIES

The following penalties as detailed out in the next sections shall apply in an event of breach of service levels as agreed.

Service Level Agreement (SLA) breach	Penalty
P1 Incidents are resolved within one hour 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 up to 60% in one contractual year thereafter termination procedures will be implemented.
Incidents are resolved within two hours and beyond 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 up to 60% in one contractual year thereafter termination procedures will be implemented.
If a Bidder misses Incident Management SLA's in any 3 consecutive months across any sites in scope	50 % of the monthly fee will be deducted.
If a Bidder 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 termination procedures	50 % of the monthly fee will be deducted.
Five or more missed SLA's across all sites in scope on or across Acquisition Management, IMACDs; Asset Management; Configuration Management; Maintenance and Repair in a measuring period	20% of the monthly fee will be deducted per invoice

Table 4: SLA breaches and penalty for incidents

The following **SLA penalties** shall apply when the Service Provider does not comply with the agreed SLA.

SLA Breach	Penalty
Failure to comply to agreed SLA	10% of contract capital value withheld

Table 5: SLA breaches and penalty for unresolved 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

4 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 Security team to discuss the following, but not limited to:

4.1 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 end	Status of new enhancements, fixes, requests	Security Team
2	Weekly Service Review Reports for open, closed incidents, 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 end.	Open and closed incidents. Status of each incident in terms of SLA. Reason of SLA breaches if any and measures that will be put in place to avoid breach.	Security Team
3	Maintenance reports: report against the maintenance schedule. This will include issues	Every day of the week and a consolidated version for all 4 weeks on the last day of the month end	Modules worked on. Issues discovered per module and how they were resolved.	Security Team

#	Report Name	Frequency	Content and Format	Submitted to
	picked up during their maintenance.		Details on any general maintenance work carried out.	
4	Monthly Systems Availability Report against the ACSA required target of 99.9 % uptime.	Last day of the month	System availability System downtime	Security Team
5	Preventative work done.	Monthly (i.e., 4th of the following month).	Report on various preventative work as per section 4.2 above.	Security Team
6	Issues for ACSA's attention.	Last day of the month	Any relevant issues that needs to be brought to ACSA's attention by the Service Provider.	Security Team
7	Ad-hoc	As and when required	Ad-hoc, depending on the request at hand.	Security Team

Table 7: Reporting Matrix

4.2 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 as stated in. 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 Minutes. Monthly Reports.	Attendance Register Minutes of meeting including updated Action items, Decisions Made, Risk & Issue Log Acceptance of deliverables
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,	Service Provider's Service Delivery Manager, Technical Resources and ACSA Security team	Minutes of Previous Meeting. Updated Risk and Issue Log.	Attendance Register. Minutes of Meeting. Acceptance of deliverables.

Frequency	Meeting Name	Standing Agenda	Participants and Role	Prior documents to be submitted by the Service Provider	Documents to be produced after meeting
		Contractual/Financial and Governance, General and all other requirements related to the services. Internal and External Audits of the Services in Scope.			
Ad-hoc	Ad-hoc	Ad-hoc	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 8: Meetings Matrix