REF: GM CM/SOC/ IT/02 /21

M/S _____

_____

_____

Sub: Establishing of Hybrid Security Operation Center (SOC)

Dear Sirs,

We are pleased to invite your sealed tenders for the item/ services mentioned above. In case of more than one schedule separate tender for each schedule should be furnished. The terms & conditions of the tender / supplies are given below:-

A) SUBMISSION OFTENDER

1. You are required to send your tenders addressed to GM Contract Management, PIA Supply Chain Management Building, JIAP Karachi latest by **21-06-2021 at 1030hrs.** The tenders may be dropped in the tender box marked as **"Tender Box Commercial Purchases"** placed at the entrance of the PIACL Supply Chain Management Building latest by **10:30** hours on the specified date. You may also send your tenders through registered A/D mail addressed to GM Contract Management, which must reach before the closing date and time mentioned above .Tenders will be opened **at 11:00 hours** the same day in the presence of tenderers.

2. Tenders received after stipulated date & time shall not be considered. The Corporation will not be responsible for postal delays. The decision of GM Contract Management in this respect shall be final and binding.

3. Bidders are required to submit a Pay Order of Rs. 6000/- (Non-Refundable) as tender fees along with Technical Proposal (Local Bidders).

B) EARNEST MONEY/ BID SECURITY (Local Bidders Only)

The Tender should be accompanied a Pay Order payable (valid for 120 days from the date of tender opening) equivalent to 2% of total bid value in the name of M/S PAKISTAN INTERNATIONAL AIRLINES as interest free Earnest Money (Refundable). Earnest Money in other shape shall not be accepted. Earnest / Security Money deposited against a running contract (s) purchase orders(s) shall not be transferable as earnest money for any other tender. All tenders without Earnest Money shall not be considered.

C) SECURITY DEPOSIT/ PERFORMANCE GUARANTEE (Local Bidders Only)

The successful tenderer upon award of Contract / Purchase Order will be required to furnish security deposit (Pay Order OR Bank Guarantee) in the amount equivalent to 10 % of total tender value stated in the Letter of Acceptance as interest free Security deposit and to remain valid 3-months after the expiry period of the Contract. The Earnest Money already held can be converted into Security Deposit and balance amount if any shall be deposited as above.

D) Instruction to Bidder

PREPARATIONOFTENDER **"Single Stage Two Envelope Basis"**

- The BID (Tender) submitted shall comprise of a single package containing two sealed envelopes, each envelope shall be marked and will contain **"TECHNICAL"** and **"FINANCIAL"** proposal.
- On the given tender opening date only **"Technical Proposal"** will be opened in the presence of tenderers available.
- The **"Financial Proposal"** shall be shown to the parties but will be retained with PIA without being opened.
- After Technical Evaluation of the received Technical Proposals, Financial Proposals will be opened publicly at the date, time & venue to be announced and will be communicated to the bidders in advance.
- PIA will open the "Financial Proposals" publicly of the parties whose Technical

Proposals have been found acceptable.

- Financial Proposals of the technically not-acceptable bids shall be remained **un-opened** till the completion of tender process.

E) PREPARATION OF TENDER - TECHNICALPROPOSAL:

All mandatory requirements are given in the schedule

Please give all the available technical details of the items offered by you, supported with the technical literature, brochure, drawings and pictures, client list details, authorization certificates etc.

BIDS / Tenders / Technical Proposal received shall be evaluated in accordance with the given technical specifications.

PIA's requirements with Technical Specifications are given.

Bidders **MUST**:

- Be registered with Sales Tax Authorities; please attach copy of Registration Certificate (Local Bidders Only).
- Quote Rates, GST, and other taxes separately.
- Bid on Prescribed Performa issued by PIA.
- Affix the company seal on all tender documents.

Mention clearly Tender Reference on **TOP RIGHT CORNER OF PROPERLY SEALED ENVELOPE, BEARING COMPANY'S STAMP**

F) PREPARATION OF TENDER – FINANCIALPROPOSAL

The tenders should be enclosed in double cover. The inner cover should be sealed having enclosed the following documents:

a) Financial Evaluation duly filled in, signed and sealed.
b) Original Pay Order for Earnest Money.
c) Undertaking on Rs. 100/= above non-judicial Stamp Paper duly signed and stamped by a Public Notary Oath Commissioner (Local Bidders Only).
d) The outer cover should bear address of the General Manager Contract Management, PIA SCM Building, Karachi Airport and reference number of the tender with opening date of tender.
e) All information about the services /material proposed to be supplied must be given as required in the schedule to tender.

G) PRICES

a) The Prices mentioned in the tender will be treated as firm till the completion of Purchase Order /Contract.
b) The Prices must be stated both in words and figures. Additional information, if any must be linked with entries on the Schedule to Tender.
c) Offers must be valid for 120 days.

H) Duration of Contract

The Agreement shall be for a term of Three (03) years from the cut-over Date. The vendor is liable to provide support services for three (03) years from the date of cutover. After three (3) years, the support agreement may be renewed for the period of one (01) year and maximum number of extensions could be two (02) subject to PIACL requirement, and subject to satisfactory performance with written mutual consent of the Parties on same terms and conditions of the present agreement or otherwise agreed between the Parties at the time of renewal.

Yours truly,

Iftikhar M. Usmani
GM Contract Management
Supply Chain Management
PIA Head Office, Karachi.
Ph: 021 9904 3081, 9904 4101
Email: khijzpk@piac.aero,
contract.administration@piac.aero

INTRODUCTION

PIAC desires to engage the firm(s) for the establishing of Hybrid Security Operation Center (SOC). This Hybrid Security Operation Center (SOC) contract will remain enforce for the period of Three (03) years. The SOC scope and specifications are mentioned in Scope of work and Annexure A.

SCOPE OF Work

The function of the hybrid security operations center (SOC) is to

- monitor,
- prevent,
- detect,
- investigate, and
- respond to cyber threats round the clock.

The SOC team will be charged with variety of technologies for ensuring that potential security incidents are correctly:

- identified,
- analyzed,
- defended,
- investigated, and
- reported

and will be responsible to protect the PIACL's assets including,

- intellectual property,
- personnel data,
- business systems, and
- brand integrity.

The SOC will implement the PIAC overall cyber security strategy and acts as the central point of collaboration in coordinated efforts to defend against cyber attacks. The SOC shall also perform vulnerability assessment once in six months and submit a report for all servers and core network devices. They shall also coordinate to relevant teams for required remedies. The SOC will also be responsible for cyber security audit review and compliance.

What shall a SOC Do?

The SOC (Security Operation Center) will be a centralized function within PIAC that will continuously monitor and improve organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents. The SOC will also be responsible to take preventive measures for PIAC Data leakages. The SOC team should be available on the offsite round the clock 24/7, led by a senior cyber-security staff (L2 support) who should be available on the PIA site on a general shift and off timing will be covered by the offsite Service Provider team.

- **Prevention and detection:** The SOC shall monitor the PIAC network round-the-clock for prevention and detection of cyber security threads. The SOC team should detect malicious activities and coordinate with relevant teams to prevent them before they can cause any damage. They shall also be responsible to gather information for a deeper investigation. The SOC team shall also perform vulnerability assessment and coordinate with relevant teams for their management.
- **Investigation:** The SOC team should analyze the suspicious activities on PIAC's network to determine the nature of the threat and the extent to which it has penetrated the infrastructure. The SOC analyst views the PIAC's network and operations from the perspective of an attacker, looking for key indicators and areas of exposure before they are exploited. The SOC combines information about PIAC's network with proposed and available tools to perform an effective triage. The SOC identifies and performs a triage on the various types of security incidents by understanding how attacks unfold, and how to effectively respond before they get out of hand.

- **Response:** The SOC shall coordinate a response to remediate the issue. As soon as an incident is confirmed, the SOC acts as first responder, coordinates with relevant teams to perform actions such as isolating endpoints, terminating harmful processes, preventing them from executing, deleting files, and more. In the aftermath of an incident, the SOC coordinates with relevant teams to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems or deploying viable backups in order to circumvent the attack. When successful, this step will return the network to the state it was in prior to the incident.

Service Provider Responsibility

The vendor shall be responsible to provide complete hybrid SOC solution with predefined scope, required IT equipment, services, software and technical resources stipulated in Annex "A"

The Service Provider

1. Shall be responsible for physical installation and configuration of all provided hardware, software, and licenses.
2. Shall monitor cyber-attacks both internal and external. Categorizing, analyzing, assigning, prioritizing, responding, and reporting events received by SOC.
3. shall be responsible to identify the gaps in PIA cyber security environment that could be exploited by threat actors and make the recommendation to PIA to fill the identified gaps.
4. Shall be responsible to ensure that vulnerabilities/weaknesses were exploited during cyber-attacks are properly mitigated to prevent same type of attacks in future.
5. Shall be responsible to ensures that all cyber threat advisories are timely reported to PIA.
6. shall be responsible to provide 24/7 L1 and L2 support. L1 support shall be covered by its off-site team round the clock 24/7. It shall depute required technical resources for L2 support and SIEM administrator on PIA premises in normal working hours (9x5 hours on working days). Service Provider shall extend L2 support for off timing by its offsite team. All technical resources offsite and onsite must be at Service provider payroll and must have the required qualifications and experience. In case of exception prior explicit approval of PIAC would be required.
7. On-site SIEM administrator will be responsible to manage SOC infrastructure including hardware and software, creation of Dashboards and reports as per PIA needs, management of log sources, integration of new logs, management and creation of filters and searches.
8. Onsite and offsite technical resources must be backed or powered by service provider's cyber security team in case of cyber threat escalation.
9. shall cover two (02) per month forensic investigations for cyber security incidents.
10. Shall be responsible to conduct 12 (Twelve) forensic investigations for cyber security incidents in one year. These forensic investigations will be calculated separately from forensic investigations mentioned in Point # 9 and will be conducted on need basis and only investigations conducted will be invoiced quarterly.
11. shall be responsible for complete system administration of SOC solution, hardware, and software. It shall also provide hardware with professional on-site support with parts and labor, next business day for 03 years, etc. In addition to it, Service provider shall also be responsible for purchase and renewals of proposed software licenses.
12. Shall be responsible to provide replacement of SOC member in case of unavailability of any SOC team member.
13. shall perform vulnerability assessment and submit a report at least once in six months for all servers and core network devices. Vulnerability assessment tools used by service provider must be renowned and must not be freeware or open-source software.
14. shall be responsible for cyber security audit review and compliance.
15. Shall provide complete support for integration of proposed SOC hardware and software with existing PIAC's environment.
16. shall be responsible to update/replace/add the equipment, hardware, software, license, human resource if need arises to smoothly run the Security operation Centre (SOC).
17. shall be responsible for providing complete security to the PIACL network, its systems, against all/any threats, including without limitation, cyber attacks, hacking, data lost due to viruses, bugs, security breaches, and attempts of unauthorized access to PIACL network by aliens etc.
18. shall be responsible for conducting both cyber security awareness session/training and system health check once a year.
19. Shall prepare & provide comprehensive documentation for installation, configuration, and integration of SOC solution in PIA's environment.
20. shall be responsible to devise and review SOC Processes and SOPs with audit teams to verify policy compliance and improve SOC performance and efficiency.
21. Shall provide SIEM & EDR additional licenses and their quantity for the second/third year or renewal of old licenses for the second/third year will be on PIA request only.
22. Shall provide Incident tracking system for at least 05 users.

PIAC Responsibility

The PIAC will be responsible to provide the following:

1. Sitting arrangement for SOC team with required equipment (PCs, power, network connectivity etc.)
2. Rack space for SOC hardware including power and network connectivity,
3. Basic support to SOC hardware and software
4. Details about PIA IT infrastructure and Escalation Hierarchy
5. Access to systems on premises or remotely. Provide VPN access for 24x7 off site monitoring of SOC.
6. PIA Email and domain accounts for SOC team, if required
7. Information related to Network Diagrams, critical assets list, privileged users list etc.

RESPONSE REQUIREMENTS

Potential bidders must follow the following requirement for their responses.

- Certificate of Company/Firm/Contractor Registration/Incorporation under the laws of Pakistan.
- Valid Registration Certificate for Income Tax & Sales Tax (GST).
- Bidder must submit earnest money and security deposit as per PIA rules.
- Incomplete and conditional responses will not be entertained.
- PIAC reserves the right to accept/reject any response or cancel the tender process altogether at any stage with assigning reason.
- Responses are liable to be rejected if; they are not conforming to the terms, conditions and specifications stipulated in this document.
- The Responses submitted via email or fax will not be entertained.

EVALUATION CRITERIA

Bidder should be vigilant:

- To fulfil all requirements as laid down in Annex-A "Technical Specifications" and Annex-C "Mandatory Requirements" of evaluation criteria.
- That proposed bid may be rejected if any of the requirement is not met in "Mandatory Requirements" and "Technical Specifications" and no further condition shall be given.
- That minimum qualifying score is 75% (in General Evaluation).

ANNEXURE A-Technical Specifications

All specifications to include " or equivalent " wherever applicable

The following are the details and Technical Specifications of SOC:

S.No	Description	Quantity
1	Security Operation Center (SOC) hardware (Server) with OS Licenses	03
2	SIEM (Security Information & Event Management) Software in HA	01
3	EDR (End Point Detection and Response)	100 x 2
4	Technical Resources for SOC	
5	Additional Forensic Per Year	12
6	Vulnerability Assessment	Once in six months
7	Awareness/Training Sessions for IT Staff	Once in a Year
8	Incident Tracking System	Five users

Technical Specification

1. Security Operation Center (SOC) hardware (Servers) with OS Licenses

The proposed hardware (Server) must include required OS licenses and storage for SOC with 3 years warranty including professional on-site next business day support with parts and labor.

PowerEdge R740/R740Motherboard or equivalent or higher	1
Chassis with up to 16 x 2.5" SAS/SATA Hard Drives for 2CPU Configuration	1
Intel Xeon Silver 4214 2.2G, 12C/20T, 9.6GT/s, 16.5M Cache, Turbo, HT (85W) DDR4 2400 or equivalent or higher	2
16GB RDIMM, 2666MT/s, Dual Rank or equivalent or higher	8
2.4TB 10K RPM Self-Encrypting SAS 12Gbps 512e 2.5in Hot-plug Hard Drive,3.5in HYB CARR, FIPS140, CK or equivalent or higher	10
iDRAC9, Express or equivalent or higher	1
PERC H730P+ RAID Controller or equivalent or higher	1
Broadcom 57416 Dual Port 10GbE BASE-T Adapter, PCIe Full Height or equivalent or higher	1
Broadcom 5720 Q Port 1 GDE BASE-T, RNDC or equivalent or higher	1
Dual, Hot-plug, Redundant Power Supply (1+1), 750W or equivalent or higher	1
DVD ROM or equivalent or higher	1
Ready Rails Sliding Rails with Cable Management Arm or equivalent	1
3Yr Pro support Next Business Day Onsite Service	1
Quantity	**03**

2. SIEM (Security Information & Event Management)

First Year	Sizing
Event Generation (Event per Second) Licenses	1000
SIEM with HA(High Availability)	
Software and support for 01 Year	

Second Year	Sizing
Event Generation (Event per Second) Licenses	1000
SIEM with HA (High Availability)	
Support Renewal of First Year Procured Licenses (Event per Second)	1000
Software and support for 01 Year	

Third Year	Sizing
Support Renewal of First & Second Year Procured Licenses (Event per Second)	2000
Software and support for 01 Year	

SIEM's must include:

- Log Collection
- Normalization – Collecting logs and normalizing them into a standard format.
- Notifications and Alerts – Notifying the user when security threats are identified.
- Security Incident Detection
- Threat response workflow – Workflow for handling past security events.

SIEM must have following core features:

- **Log Data Management**

SIEM must have log data management component, which can pool log data from a variety of different sources, each with their own way of categorizing and recording data. It must have ability to normalize data effectively. The proposed SIEM system can recognize patterns from pool data of malicious behavior and raise notifications to alert the user to take action.

- **Correlation**

The proposed solution must have capability to look for common trends and attributes that would link different events together so that meaningful and useful information may be derived.

- **Compliance Reporting**

The proposed SIEM solution must have extensive compliance reporting features. It must have onboard report generating system that will help to generate different reports.

- **Threat Intelligence**

The proposed solution must have some sort of threat intelligence that can generate reports in detail how attack/breach happened extensively. The proposed solution must also have ability to set the criteria for future security threats on the basis of threat intelligence.

- **Retention**

The Proposed solution must have capability to address how the data and events are stored in the long run, as well as what to do with historical data.

- **Dashboard**

The proposed solution must have customizable dashboard with visualization.

It must support Windows, Linux, DNS, IIS, Oracle, Ms. SQL, EBS, syslog, sftp, ftp, network devices (Cisco, Huawei), etc.

3. End Point Detection and Response (EDR)

Description First Year	Sizing
End Point Detection and Response (EDR) Solution Licenses	100
Software Subscription and support for 01 Year	

Description Second Year	Sizing
End Point Detection and Response (EDR) Solution New Licenses	100
End Point Detection and Response (EDR) Solution First Year License renewal	100
Software Subscription and support for 01 Year	

Description Third Year	Sizing
End Point Detection and Response (EDR) Solution License renewal	200
Software Subscription and support for 01 Year	

Proposed EDR MUST be "Off-the-Shelf", commercially available, renowned and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment).It must not be freeware.

1. The solution must have a unified policies, centralized reporting, and tasks execution within a Single-console for centralized management – on-prem.
2. Suggested solution management server must have ability to send logs to SIEM, SYSLOG servers etc.
3. The solution must have different administrators functions that have a single interface/dashboard during sign on and controlled by privileges and rights based on their functions (Administrator, Reviewer, Investigator, etc.).
4. The suggested solution must support secure communication between management console and endpoints with EDR agent.
5. The solution should be able to send email notifications when certain types of security alerts are generated.
6. The proposed EDR must have advance and modern features available.
7. The proposed EDR must have advance detection, visibility, and response features.
8. The proposed solution must be without Sandboxing.
9. The proposed solution must allow the creation of accounts with different roles used to administer the solution, just monitor the alerts, or review changes.
10. The solution must support backup and restore.

4. Technical Resources for SOC

Service Provider shall provide the following resources to PIAC to perform the defined SOC functions on-premises:

Technical Resources/Function On-site	Quantity
Senior Cyber-Security Personnel (L2 Support) (9x5) working days	01
SIEM Administrator (System Administrator)(9x5) working days	01

Following are the technical specifications of the required resources:

Senior Cyber-Security Personnel (L2 Support) – Qty - 01

The Senior cyber-security (Team Lead) must

- Be IT graduate
- Be Certified cyber-security specialist.
- have SOC /SIEM related certifications such as SIEM Analyst, SIEM administration, Incident response etc.
- At least 03 years of cyber-security experience
- Have at least 02 years of experience to lead the Security Team/SOC
- have ability to perform deep-dive incident analysis.
- have ability to perform analysis of the incidents.
- have leverage cyber-attacks, indicators, and correlations to identify potential threats.
- have strong knowledge/skills to identify gaps and leads in implementation of new methods and technologies to sufficiently detect emerging cyber threats.
- have experience to perform forensics and malware analysis and identification of Indicators of Compromise (IOCs) to evaluate incident scope and associated impact in support of identification of security incidents.

- provide recommendations to enhance and advance the defensive capabilities based upon the research and cyber threat feeds.
- Provide assistance for IOCs (Indicators of Compromise) based on the emerging threats to cyber world and to build use cases accordingly.

SIEM Administrator – Qty - 01

The SIEM Administrator must

- be IT graduate.
- be at least 01 years working experience on SIEM Software.
- have capability to detect Incidents by monitoring the SIEM interface, Rules, Reports and Dashboards
- have capability to Monitor the SIEM console resources to identify any anomalies.
- Have capability to ensure that a technical summary of the incident is prepared which includes basic analysis / categorization /priority /impact of the incident, and information required for upper-level Analysis.
- Have capability to monitor Health Checkups and provide recommendation.
- Have capability to manage SOC infrastructure including hardware and software.
- have capability for management and creation of Dashboards, Reports as per needs
- have capability for monitoring of log sources and report if any of the log source is not working.
- have capability to integrate new log sources as per the requirement.
- Capability for the Management and creation of filters and searches as per needs.
- have experience of different Operating Systems like Windows, Linux, and Unix.

The following functions of SOC will be performed from off-site by the Service Provider's shared resources:

Technical Resources/Functions Off-site	Quantity
SOC Level 1 (L1) Support (24x7)	Off site
Senior Cyber-Security Personnel (L2 Support) Off timing	Off site
SOC Level 3 (L3) Support for Forensic	Off site (at least 02 cases per month)
Onsite & Offsite teams backed by Service Provider's Cyber Security Team	Off site

a) <u>SOC Level 1 (L1) Support (24x7)</u>

- The SOC team (L1 support) shall be available offsite (Service Provider Premises) round the clock 24/7, led by a senior cyber-security specialist (L2 support) who should be available on PIA site in general shift with SIEM Administrator.

b) <u>Senior Cyber-Security Personnel (L2 Support) Off timing</u>

- Service Provider shall extend L2 support for off timing by its offsite team.

c) <u>SOC Level 3 (L3) Support for Forensic</u>

- The Service Provider shall cover at least two (02) per month forensic investigations (Level 3 support) for cyber security incidents.

d) <u>Onsite & Offsite teams backed by Service Provider's Cyber Security Team</u>

- All onsite and offsite technical resources must be backed or powered by the service provider's cyber security team in case of cyber threat escalation.

5. Additional Forensic Per Year

Description	Quantity
Forensic Per Year (if required)	12

The Service Provider shall cover two (02) per month forensic investigations for cyber security incidents which are covered in Technical Resources for SOC. In addition, Service provider will be responsible to conduct 12 (Twelve) forensic investigations for cyber security incidents in one year (if required) that will be calculated separately from forensic investigations two (02) per month and will be conducted as by need. Only investigations conducted will be invoiced quarterly. The Service Provider must add the price of 12 additional forensics per year in the financial proposal.

6. Vulnerability Assessment

The Service Provider shall perform vulnerability assessment and submit a report on at least quarterly basis for all servers (OS, applications, Databases etc. including Windows, Linux, .Net, IIS, EBS, etc) and core network devices. They shall also coordinate to relevant teams for required remedies.

Vulnerability assessment tools used by the service provider must be renowned and must not be freeware or open-source software.

Following is the tentative list of OS, Apps, DBs and Network devices:

Description	Quantity
Operating systems (OS)	100
Applications (Apps)	50
Databases (DBs)	30
Network Devices	40

7. Awareness / Training Sessions for IT Staff

The Service Provider shall be responsible for conducting cyber security awareness session/training for IT technical staff (System Administrators, Network Administrators, Developers, Database Admin &Dev and IT support engineers etc.) once a year. Awareness / Training Session must include but not limited to current ongoing cyber security trends, best practices, tools, preferred configurations (OS, applications, databases, Network etc.).

8. Incident Tracking System

The Service Provider shall be responsible to provide an incident tracking system for at least five (05) users to log and track the security incidents.

Description	Users
Incident Tracking System	05

ANNEXURE C-EVALUATIN CRITERIA

Mandatory Requirements

S.No.	Description	Documents
1	Proposed SIEM and EDR Solution MUST be "Off-the-Shelf", commercially available and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). It must not be freeware.	
2	The proposed SIEM solution MUST have a complete backup and restore capability.	Documentary Evidence
3	The Service Provider must be OEM or OEM certified Partner for the proposed SIEMsolution.	Partnership letter from OEM
4	Complete SOC solution must be offered by single service provider.	
5	Service Provider must have at least 05 years of experience to provide SOC (Security Operation Center) services or managed security services.	Provide documentary evidence
6	The service provider currently must be providing SOC services with offsite level 1, Level 2 and Level 3 to five (05) clients having 1000 EPS or higher.	Provide Client List
7	All proposed warranties and licenses of offered hardware and software must be procured for PIAC by Service Provider	
8	The proposed equipment (hardware) should not be refurbished and must have 03 years of warranty including onsite professional support next business day with parts and labour.	
9	GST, NTN and SECP registration certificate	Relevant certificates
10	Quote the Unit Rate and GST (If applicable) **SEPARATELY**	Tender Document (Financial)
11	Must be active taxpayer	
12	Company must have geographical presence in Karachi and Islamabad. More locations will be an added advantage.	Office addresses
13	Must submit technical proposal in hard paper and on CD/USB etc.	
14	OEM must be in Gartner 2020 **Leaders** for the proposed SIEM solution.	

General Requirements

S.No.	Description	Marks	Documents
1	Geographical Presence	1 Locations = 5 Marks Max = 15	Offices' addresses
2	Availability of Technical Staff(Company Technical Strength) (relevant category Support Level 1 + Support Level 2 + Support Level 3)	oneLevel 1 Support Staff = 1, max = 6 One Level 2 Support Staff = 2, max = 6 One Level-3 Support Staff = 4, max = 8 Marks Max = 20	Staff List+ CVs of Technical Staff
3	Financial Strength (Annual Turnover)	10 Million= 1 Mark Max = 15	Last two years audited reports *Evaluation will be on the basis of 2020
4	Number of years in business	5Years= 3 Marks On additional each year = 3 Marks Max = 15	Company registration certificate
5	Similar projects or Cyber Security Services successful delivery in last five years (SLA/PO at least 02 Million)	1 Project/Delivery = 1 Marks Max = 10	Purchase Orders
6	Presentation	Max = 75	

Total Marks: 150
Passing / Qualifying marks = **75%** of the total
Bidders securing Less than 75% will not be entertained further.

Financial Bid Format-

S.No.	Description	Solution Cost Including All Items with Required Quantity and support, PKR	Tax(if Applicable___% & amount), PKR	Total Cost Including All Items with Required Quantity including Tax, PKR
1	First Year			
2	Second Year			
3	Third Year			
	Total			

DRAFT AGREEMENT

This Agreement (hereinafter called the "Agreement") is made on the _____ (hereinafter called "Effective Date").

BY & BETWEEN

Pakistan International Airlines Corporation Limited, a Public Limited Company incorporated and governed under the laws of Pakistan having its Head Office at PIA Head Office Building Jinnah International Airport, Karachi, (hereinafter referred to as the "Company" and /or "PIACL" which expression shall where the context so admits include its successors and assigns) of the ONE PART

AND

Service Provider , incorporated and functioning under laws of Pakistan and having its registered office at Service Provider Address (hereinafter referred to as **"SERVICE PROVIDER",** which expression shall, wherever the context so permits, means and include its successors-in-interest, representatives and assigns),;

PIACL and **Service provider**_ shall hereinafter individually be referred as a **"Party"** and collectively as **"Parties"** where the context of this Agreement so required**.**

WHEREAS

PIACL acquired **Security Operation Centre (SOC) Solution for strengthening its cyber Security posture**

a. through tendering process
b. Service Provider**,** selected as result of competitive bidding process, shall provide **SOC solution** as per the terms agreed in the RFP and Agreement.

NOW THEREFORE THIS AGREEMENT WITNESSED AND IT IS HEREBY AGREED BETWEEN THE PARTIES AS UNDER;

1. **INTERPRETATION**

1.1 The schedule and any addendums thereon, to this Agreement shall be deemed to be a part of this Agreement.

1.2 The singular includes the plural and vice versa;

1.3 All headings are for convenience only and shall not constitute a part of, or be used in constructing, this Agreement.

1.4 Definitions:
Effective Date:- The date when the contract will become effective

Cutover Date:- The first date/day from which SOC (Security Operation Center) will go-live after receiving the acceptance certificate from PIACL. The Support service period will start from this date.

Acceptance Certificate:- Will be issued by PIACL after testing and verifying the successful installation and commissioning of SOC infrastructure, hardware, software, software licenses and human resources for Security Operation Centre (SOC) as per term agreed in RFP and agreement.

2. **CONFIDENTIALITY STATEMENT**

-

From time to time during the performance of this Agreement, it will be necessary for the Parties to provide each other with confidential information. Confidential information means and includes information and data transferred from one Party to the other under this Agreement that must be treated by the receiving Party as confidential as the receiving Party is aware or should reasonably be aware it is confidential. Confidential information includes digital, electronic, oral and visual information. Confidential information is and shall at all times remain the property of the disclosing Party. No use of any confidential information is permitted except as provided herein and no grant under any proprietary rights is hereby given or intended. In summary For purposes of this Agreement, Confidential Information means all information (in whatever format and however obtained) which: (i) relates to this Agreement; (ii) is designated as confidential by either Party; or (iii) relates to the business, affairs, networks, customers, products, developments, trade secrets, know-how and personnel of either Party (including customer data) and which may reasonably be regarded as confidential information of the disclosing Party. Confidential Information does not include any information which: (i) is in the public domain at the time of disclosure or becomes available thereafter to the public without restriction and not as a result of the act or omission of the receiving Party; (ii) is rightfully obtained by the receiving Party from a third party without restriction as to

disclosure, or (iii) is lawfully in the possession of the receiving Party at the time of disclosure and not otherwise subject to restriction on disclosure.
In this regard the parties shall:

2.1 Keep and maintain in the strictest confidence all such confidential information and not disclose the same to any third party, except as authorized in advance by the original disclosing Party in writing;

2.2 Restrict disclosure of confidential information to employees who have a "need to know" the same in performing under the Agreement. Such confidential information shall be handled with a high degree of care;

2.3 Use confidential information only as required in the performance of the Agreement;

2.4 Prior to disclosing any confidential information in accordance with any due legal process or the rules of any Stock Exchange, the Party intending to make such disclosure shall immediately notify the other Party to enable such other Party to seek a protective or exemption order. Prior to making any such disclosure, the Party intending to make such disclosure shall allow the other Party to review the same;

2.5 Confidential information shall be considered confidential after termination or expiration of the agreement unless PIACL provides consent letter to service provider for declassification of its information.

2.6 The obligation to maintain confidentiality shall not apply to disclosures required to be made by either party in compliance with any applicable laws, rules or regulations or fulfilment of any directives or instructions by any regulatory authority or compliance with any judgment order or decree of any court of competent jurisdiction.

This work contains confidential information and proprietary information belonging to Service Provider and PIACL. This confidential information is to be used by both Parties only for the purpose for which it is supplied. Neither Party shall disclose the confidential information to any third party without the prior written consent of the Disclosing party. The obligation for maintaining the confidentiality of the information shall survive the termination or expiry, as the case is, of this Agreement.

Parties agrees that in the event of any violation of the duty of confidentiality and such violation constitutes a fundamental breach of this Agreement and shall result in grave and serious injury and damage to the other party and that no monetary damages can compensate such injury and damages. The matter shall be settled as per dispute resolution clause of this agreement.

Each Party further agrees, upon expiration or earlier termination of this Agreement for whatever cause, all Confidential Information disclosed hereunder, including copies thereof, shall be returned to the disclosing party within three (3) working days from the date of such termination or expiration, or if the disclosing party instructs the Confidential Information to be destroyed, the receiving party shall sign a declaration certifying that all the related Confidential Information has been destroyed within three (3) working days thereof.

3. WARRANTIES AND REPRESENTATIONS BY SERVICE PROVIDER

Through this Agreement, the Service provider hereby warrants and undertakes to PIACL, that it has requisite professional expertise and necessary infrastructure, hardware, software, all licenses, and human resources to provide SOC solution requirements of PIACL and related services to the complete satisfaction of PIACL. Moreover, the Service provider will also be responsible for all warranties and guaranties for the human resources to be deployed, equipment to be purchased, services to be provided, software and their licenses to be acquired in the favor of PIACL. The service provider will also be responsible for any claim of damages in case of faulty and malfunctioning of products, services, software and hardware and inexperienced human resources.

3.1 Service Provider warrants and represents that the design shall strictly follow the requirements for the services contemplated under this Agreement and that it shall provide to PIACL a solution under this Agreement that is reliable, robust and secure due to sensitivity of the data through its use of proven solutions. Service provider further warrants that the manageability and security is built within the network architecture as a function of the hardware and design rules and is designed into all Service Provider networks and derived services as a basic requirement.

4. SCOPE OF WORK

The function of the hybrid security operations center (SOC) is to

- monitor,
- prevent,
- detect,
- investigate, and
- respond to cyber threats round the clock.

The SOC team will be charged with variety of technologies for ensuring that potential security incidents are correctly:

- identified,
- analyzed,
- defended,
- investigated, and
- reported

and will be responsible to protect the PIACL's assets including,

- intellectual property,
- personnel data,
- business systems, and
- brand integrity.

The SOC will implement the PIAC overall cyber security strategy and acts as the central point of collaboration in coordinated efforts to defend against cyber attacks. The SOC shall also perform vulnerability assessment once in six months and submit a report for all servers and core network devices. They shall also coordinate to relevant teams for required remedies. The SOC will also be responsible for cyber security audit review and compliance.

What shall a SOC Do?

The SOC (Security Operation Center) will be a centralized function within PIAC that will continuously monitor and improve organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents. The SOC will also be responsible to take preventive measures for PIAC Data leakages. The SOC team should be available on the offsite round the clock 24/7, led by a senior cyber-security staff (L2 support) who should be available on the PIA site on a general shift and off timing will be covered by the offsite Service Provider team.

- **Prevention and detection:** The SOC shall monitor the PIAC network round-the-clock for prevention and detection of cyber security threads. The SOC team should detect malicious activities and coordinate with relevant teams to prevent them before they can cause any damage. They shall also be responsible to gather information for a deeper investigation. The SOC team shall also perform vulnerability assessment and coordinate with relevant teams for their management.

- **Investigation:** The SOC team should analyze the suspicious activities on PIAC's network to determine the nature of the threat and the extent to which it has penetrated the infrastructure. The SOC analyst views the PIAC's network and operations from the perspective of an attacker, looking for key indicators and areas of exposure before they are exploited. The SOC combines information about PIAC's network with proposed and available tools to perform an effective triage. The SOC identifies and performs a triage on the various types of security incidents by understanding how attacks unfold, and how to effectively respond before they get out of hand.

- **Response:** The SOC shall coordinate a response to remediate the issue. As soon as an incident is confirmed, the SOC acts as first responder, coordinates with relevant teams to perform actions such as isolating endpoints, terminating harmful processes, preventing them from executing, deleting files, and more. In the aftermath of an incident, the SOC coordinates with relevant teams to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems or deploying viable backups in order to circumvent the attack. When successful, this step will return the network to the state it was in prior to the incident.

Service Provider Responsibility

The vendor shall be responsible to provide complete hybrid SOC solution with predefined scope,

required IT equipment, services, software and technical resources stipulated in Annex "A"

The Service Provider

23. Shall be responsible for physical installation and configuration of all provided hardware, software, and licenses.
24. Shall monitor cyber-attacks both internal and external. Categorizing, analyzing, assigning, prioritizing, responding, and reporting events received by SOC.
25. shall be responsible to identify the gaps in PIA cyber security environment that could be exploited by threat actors and make the recommendation to PIA to fill the identified gaps.
26. Shall be responsible to ensure that vulnerabilities/weaknesses were exploited during cyber-attacks are properly mitigated to prevent same type of attacks in future.
27. Shall be responsible to ensures that all cyber threat advisories are timely reported to PIA.
28. shall be responsible to provide 24/7 L1 and L2 support. L1 support shall be covered by its off-site team round the clock 24/7. It shall depute required technical resources for L2 support and SIEM administrator on PIA premises in normal working hours (9x5 hours on working days). Service Provider shall extend L2 support for off timing by its offsite team. All technical resources offsite and onsite must be at Service provider payroll and must have the required qualifications and experience. In case of exception prior explicit approval of PIAC would be required.
29. On-site SIEM administrator will be responsible to manage SOC infrastructure including hardware and software, creation of Dashboards and reports as per PIA needs, management of log sources, integration of new logs, management and creation of filters and searches.
30. Onsite and offsite technical resources must be backed or powered by service provider's cyber security team in case of cyber threat escalation.
31. shall cover two (02) per month forensic investigations for cyber security incidents.
32. Shall be responsible to conduct 12 (Twelve) forensic investigations for cyber security incidents in one year. These forensic investigations will be calculated separately from forensic investigations mentioned in Point # 9 and will be conducted on need basis and only investigations conducted will be invoiced quarterly.
33. shall be responsible for complete system administration of SOC solution, hardware, and software. It shall also provide hardware with professional on-site support with parts and labor, next business day for 03 years, etc. In addition to it, Service provider shall also be responsible for purchase and renewals of proposed software licenses.
34. Shall be responsible to provide replacement of SOC member in case of unavailability of any SOC team member.
35. shall perform vulnerability assessment and submit a report at least once in six months for all servers and core network devices. Vulnerability assessment tools used by service provider must be renowned and must not be freeware or open-source software.
36. shall be responsible for cyber security audit review and compliance.
37. Shall provide complete support for integration of proposed SOC hardware and software with existing PIAC's environment.
38. shall be responsible to update/replace/add the equipment, hardware, software, license, human resource if need arises to smoothly run the Security operation Centre (SOC).
39. shall be responsible for providing complete security to the PIACL network, its systems, against all/any threats, including without limitation, cyber attacks, hacking, data lost due to viruses, bugs, security breaches, and attempts of unauthorized access to PIACL network by aliens etc.
40. shall be responsible for conducting both cyber security awareness session/training and system health check once a year.
41. Shall prepare & provide comprehensive documentation for installation, configuration, and integration of SOC solution in PIA's environment.
42. shall be responsible to devise and review SOC Processes and SOPs with audit teams to verify policy compliance and improve SOC performance and efficiency.
43. Shall provide SIEM & EDR additional licenses and their quantity for the second/third year or renewal of old licenses for the second/third year will be on PIA request only.
44. Shall provide Incident tracking system for at least 05 users.

PIAC Responsibility

The PIAC will be responsible to provide the following:

8. Sitting arrangement for SOC team with required equipment (PCs, power, network connectivity etc.)
9. Rack space for SOC hardware including power and network connectivity,
10. Basic support to SOC hardware and software
11. Details about PIA IT infrastructure and Escalation Hierarchy

12. Access to systems on premises or remotely. Provide VPN access for 24x7 off site monitoring of SOC.
13. PIA Email and domain accounts for SOC team, if required
14. Information related to Network Diagrams, critical assets list, privileged users list etc.

5. **DELIVERY TIMELINES**

Establishment of SOC and all services mentioned in the Scope of Work and RFP shall be fully commissioned, tested, and handed over to the complete satisfaction of PIACL within 45 working days at most after PO issuance. Work shall only be accepted by the PIACL upon the issuance of written certification in this regard by PIACL to Service Provider.

6. **DURATION AND TERMINATION**

The Agreement shall be for a term of Three (03) years from the cut-over Date. The vendor is liable to provide support services for three (03) years from the date of cutover. After three (3) years, the support agreement may be renewed for the period of one (01) year and maximum number of extensions could be two (02) subject to PIACL requirement, and subject to satisfactory performance with written mutual consent of the Parties on same terms and conditions of the present agreement or otherwise agreed between the Parties at the time of renewal.

6.1 For Convenience: PIACL, by written notice sent to service Provider, may terminate the contract in whole or in part at any time for its convenience giving three months prior notice. The notice of termination may specify that the termination is for convenience the extent to which Service Provider's performance under the contract is terminated and the date upon which such termination become effective. PIACL shall consider request of the service Provider for pro-rata payment till the date of termination.

6.2 For Insolvency: PIACL at any time may terminate the contract by giving written notice to Service Provider, if Service provider becomes bankrupt or insolvent. Including this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to PIACL under the agreement.

6.3 For Non-Performance: PIACL reserves its right to terminate the contract in the event of Service Provider repeated failures (say more than 3 occasions in a quarter to maintain the service level prescribed by PIACL).

7. **PERFORMANCE GAURANTEE AS SECURITY DEPOSIT**

Prior to the signing of this Agreement the Service Provider shall deposit in shape of pay order or Bank Guarantee in favor of PIACL (10% of total contract value) as interest free security deposit in lieu of Performance Guarantee with the Authorized Office of PIACL. PIACL shall have the right to recover / adjust all liabilities and/or outstanding amounts of the Service provider from the amount of Security Deposit furnished/deposited by Service Provider. The Interest Free Security Deposit shall remain with PIACL after three months of the expiry/termination of Agreement and the same will be refunded to the Service Provider after deduction of all the outstanding amounts and/or dues recoverable from Service Provider in relations to, arising out of and/or connected with this agreement. However, an amount, equal to the deducted amount from the Security Deposit, shall be deposited by Service provider within 15 days' time with PIACL to maintain the amount of Security Deposit to the level of 10% of the total contract value. In addition, PIACL shall always be entitled to recover any other amount outstanding against the Service Provider through different modes and methods provided under the applicable laws.

8. TAXES AND DUTIES

The Service provider shall be entirely responsible for all taxes, duties and other such levies imposed on by the concerned authorities such as but not limited to Income Tax and Sales Tax Department or any other relevant authority on any payment made by PIACL under this agreement or otherwise.

9. SAFETY & SECURITY

Service provider shall comply with all laws, rules, regulations, notifications and standing instructions issued by Government, Semi Government or Local Bodies and shall take safety measures and make appropriate arrangements for safety of men and materials in carrying out the work under this Agreement. Any beach thereof will invoke immediate termination of contract and/or claim of damages by PIACL from Service Provider.
The Service Provider shall always be responsible for the conduct and behavior of all its

employees and the persons deployed for the provision of service hereunder and shall at all times ensure that no such employee or person shall commit any misconduct himself or be a nuisance or negligent in the provision of the Services or act or behave against the interests of or in a manner not beneficial for the PIACL. The Service Provider shall ensure that none of its employee or person assigned for the provision of Service hereunder have a police record for any criminal activities or have ever been convicted in any court of law for any criminal act committed by them. The Service Provider shall ensure and provide such adequate documentary evidence to the PAICL with regard to the Police clearance of its employees. Also, the Service Provider shall manage & prepare ID Cards of its own cost and expenses of its employees in accordance with the format provided by the PIACL and security policy. It is clarified that such information will be required by the PIACL for security purpose.

10. GENERAL TERMS AND CONDITIONS

10.1 Service Provider warrants that the services shall be performed in a professional manner consistent with best industry standards, internationally accepted and applicable to such services.

10.2 Service Provider shall be responsible for the payment of all the taxes, dues etc. under the law in respect of any and all person working for or on behalf of Service Provider as a part of the team within PIACL premises.

10.3 Service Provider shall ensure the commissioning and support/maintenance of the services as contemplated under this Agreement in a timely manner and to the complete satisfaction of PIACL. However, in case, of any delay caused in commissioning or support due to Force Mejure shall be honored.

10.4 Any mishap occurring due to conditions or resources not in control of Service Provider or PIACL cannot be made a liability against either party

11. NOTICES

11.1 All notices, requests, or other communications hereunder shall be in writing, addressed to the parties as follows:

To PIACL: **The General Manager Infrastructure** Address: Room # 1, PIA Computer Center, Terminal-1, Karachi Airport, PIACL Head Office, Karachi	To Service Provider: **The Service provider GM** Service provider Address.

11.2 Notices mailed by registered or certified mail shall conclusively be deemed to have been received by the addressee, when delivered. Notices sent by telex or fax shall be conclusively deemed, to have been received by the addressee upon confirmation of receipt. The other party shall be informed through written notice of the change of address, telephone, telex, fax and/or email immediately.

12. **DISPUTE RESOLUTION AND GOVERNING LAW**

12.1 The Parties shall endeavor to resolve any difference, dispute or matter arising under this Agreement, failing which either Party may refer it to arbitration before a mutually appointed sole arbitrator. The arbitration shall be conducted in accordance with the Arbitration Act, 1940 and the venue for arbitration shall be at Karachi.

12.2 This Agreement shall be governed by the laws of Islamic Republic of Pakistan. The parties hereby irrevocably consented to the exclusive jurisdiction of courts at Karachi Pakistan to atry any matter arising out of, connected with and in relation to this agreement.

13. **INDEMNITY**

The Service Provider undertakes and agrees to indemnify and hold harmless PIA, its officers and agents from and against all claims, demands, liabilities, damages and expenses of any nature whatsoever, arising out of, resulting from and in connection with this agreement whether due to performance / non-performance or poor performance of any services under this Agreement by the Service Provider, its employees or its agents or otherwise. In any case, the obligation

on the part of the Service Provider to indemnify shall not be limited to the contract value where cause(s) giving rise to any such claim, demand, liability, damage, expenses etc are proven to have been attributed beyond doubt solely to the actions/breeches/violations/non, poor and under performance of the Service Provider.

14. FORCE MAJEURE

This Agreement shall be suspended during the period and to the extent of such period that either parties are prevented or hindered from complying with their obligations under any part of this Agreement by any cause beyond their reasonable control, including , acts of God, governmental authority, unavailability energy sources and natural disasters or weather related outages. If such period of suspension exceed **30** days, the Agreement shall immediately terminate unless the parties otherwise agree in agreement and advance paid amounts for unexpired (payments if any) shall be refunded to PIACL.

15. PENALTY

In case of non performance, poor and under performance and defaults attributable to the Service Provider and/or its staff, of the requirements/ conditions as stated in the agreement, scope of work, RFP and service level requirement and any deviation from the contents of the same may invoke penalties at per occurrence formula, which will be as follows:

15.1 In case of non-satisfactory performance referred in Service Level Requirements (Point 16), scope of work (Point 4) and RFP (Annex A), 10% of the service charges of one quarter shall be deducted on each incident.

15.2 In case of non-satisfactory performance referred in the rest of the clauses of agreement, 10% of the total amount of agreement shall be deducted on each deviation.

16. SERVICE LEVEL REQUIREMENTS

- Maximum SOC service up time: 99.8% in One quarter.
- Time and Level of on-site service coverage:
  - 09:00 AM to 05:30 PM (Working days) by SIEM Administrator.
  - 09:30 AM to 05:30 PM (Working days) by Senior Cyber security Specialist (L2 Support).
- Time and Level of off-site service coverage:
  - off-site SOC monitoring 24/7 by Cyber Security Specialist (L1 Support).
  - Off-site Senior Cyber security specialist (L2 support) of SOC for off timing.
  - Off site SOC Level 3 (L3 Support) for Forensic investigation, etc. 02 cases per month.
- All deputed technical resources must be backed or powered by cyber security team off-site in case of cyber threat escalation. The Service provider will provide escalation Matrix.
- Audit Compliance: 99%.
- gap Analysis : Once in six months
- Awareness session/training : Once in a year
- System health check : Once in year
- Vulnerability Assessment: Once in six months.

S.No	Cyber Attack Severity Level	Impact	Detection Time or Alert Time	Response or Repair Time after Detection/Alert
1.	Critical I	Affects large number of systems or users on customer site and interrupts business or service delivery or damages reputation.	30 Minutes	1 Hour
2.	Major II	Affect a few staff and interrupt business to some degree	30 Minutes	2 Hours
3.	Minor III	Affect a few staff but does not interrupt business	1 Hour	3 Hours

16.1 SEVERITY LEVEL & RESPONSE TIME

17. VARIATION AND AMENDMENT

This Agreement shall not be varied, modified, altered, amended or supplemented etc. except through mutual consent of both parties in writing.

18. SCHEDULES / ANNEXURES

For all intents and purposes, the Schedules/Exhibits of this Agreement shall form an integral part of this agreement and the contractor shall comply with and fulfill all the terms and conditions stipulated in such schedules and exhibits. Any default by the contractor to comply with any terms and conditions incorporated in the schedules /exhibit shall be deemed as breach of this Agreement.

19. PAYMENT TERMS

Payment will be made as follows:

- **First year:** The Service provider will be eligible for 60% of total amount after cutover date and 10% of total amount on completion of each quarter of first year of contract term after cutover date.
- **Second Year:** The Service Provider will be eligible for 40% of total amount at the start of first quarter and 15% on the completion of each quarter of second Year of contract term.
- **Third Year:** The Service Provider will be eligible for 40% of total amount at the start of first quarter and 15 % of total amount on the completion of each quarter of third Year of Contract term. PIACL (Customer) and Service Provider Shall bear/pay their respective taxes in case there would be any tax variation by Government of Pakistan during agreement period stipulated in this document.

20. TRANSFER OR ASSIGNMENT

- The Service shall not assign or sub-contract its obligations under the Contract, in whole or in part, except with the PIACL prior written consent. In case of written consent by PIACL, all the expenses of assignment shall be borne by Agency including without limitation lawyers fee without any change in the terms of this contract, unless consented by the PIACL.

- The Service Provider shall guarantee that any and all assignees / subcontractors of the Service Provider shall, for performance of any part / whole of the services under the contract, comply fully with the terms and conditions of the Contract applicable to such part / whole of the services under the contract.
- If the Service Provider assigns this Agreement to any other party in contravention of this Article, PIA in its discretion may terminate this agreement and / or black list and debar the Agency for future to execute any contract with PIA with confiscation of Security Deposit and/or claim damages through legal recourse.

21. WAIVER

The failure of either at any time to require the performance by the other of any of the terms and provisions hereof shall in no way effect the right of that party thereafter to enforce the same nor shall the waiver by either party or any breach of the terms or provision hereof taken or held to be waiver of any succeeding breach of any such terms or provision itself.

22. FORFEITURE OF INTEREST FREE PERFORMANCE SECURITY

- The Interest Free Performance Security/Security Deposit shall be forfeited by PIACL, on occurrence of any / all of the following conditions:
  - If the Service Provider commits a default under the Contract.
  - If the Service Provider fails to fulfill any of the obligations under the Contract.
  - If the Service Provider violates any of the terms and conditions of the Contract.
- The Service Provider shall cause the validity period of the performance security to be extended for such period(s) as the contract performance may be extended. In case the Service Provider fails to submit Security Deposit with extended validity period for such period(s) as the contract performance may be extended, an amount equal to 10% of total contract value shall be deducted from the payments to be made against the contract.
- If the Service Provider fails / poor/ delays in performance of any of the obligations, under the Contract / violates any of the provisions of the Contract / commits breach of any of the terms and conditions of the Contract the PIACL may, without prejudice to any other right of action / remedy it may have, forfeit Performance Security/Security Deposit of the Service Provider.
- Failure to supply required deliverable/ services within the specified time period will invoke penalty as specified in this document. In addition to that, Performance Security amount will be forfeited and the Service Provider will not be allowed to participate in future tenders as well.

Now this agreement witnesses that in consideration of the mutual covenants herein contained, the Parties hereto have caused this Agreement to be signed in their respective names in two identical counterparts each of which shall be deemed as original as the day, month and year first above written.

This agreement is agreed and reviewed by following:

_____ _____

WITNESSES:

_____ _____

General Manager Contract Management **General Manager IT Infrastructure**

INTEGRITY PACT / DISCLOSURE CLAUSE

(To be submitted on Company's Letterhead)

Declaration of Fees, Commissions and Brokerage Etc. Payable by the Suppliers, Vendors, Distributors, Manufacturers, Contractor & Service Providers of Goods, Services & Works_____ the Seller / Supplier / Contractor hereby declares its intention not to obtain the procurement of any Contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative sub-division or agency thereof or any other entity owned or controlled by it (GOP) through any corrupt business practice.

Without limiting the generality of the forgoing the Seller / Supplier / Contractor represents and warrants that it has fully declared the brokerage, commission, fees etc., paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback whether described as consultation fee or otherwise, with the object of obtaining or including the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from Government of Pakistan, except that which has been expressly declared pursuant hereto.

The Seller / Supplier / Contractor certifies that it has made and will make full disclosure of all agreements an arrangements with all persons in respect of or related to the transaction with Government of Pakistan and has not taken any action or will not take any action to circumvent the above declaration, representation or warranty.

The Seller / Supplier / Contractor accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall without prejudice to any other right and remedies available to Government of Pakistan under any law, contract or other instrument, be void-able at the option of Government of Pakistan.

Notwithstanding any rights and remedies exercised by Government of Pakistan in this regard, the Seller / Supplier / Contractor agrees to indemnify Government of Pakistan for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to Government of Pakistan in any amount equivalent to ten time the sum of any commission, gratification, brief, finder's fee or kickback given by the Seller / Supplier / Contractor as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever from Government of Pakistan.

(To be submitted on Rs. 100 Stamp Paper)

General Manager Contract Management
Supply Chain management
Pakistan International Airlines
Karachi

Subject: **Undertaking to Execute Contract**

Dear Sir,

1. We/I, the undersigned tenderer do hereby confirm, agree and under take to do following in the event our/my tender for supply of
   _____
   _____to PIACL is approved and accepted:

2. That we / I will into and execute the formal contract, a copy of which has been supplied to us / me, receipt whereof is hereby acknowledge and which has been studied and under stood by me / us without any change, amendment, revision or addition thereto, within a period of seven days when required by PIACL to doso.

3. That all expense in connection with the preparation and execution of the contract including stamp duty will be borne by us /me.

4. That we / I shall deposit with PIA the amount of security as specified in the contract which shall continue to be held by PIACL until three months after expiry of the contract period.

5. That in event of our / my failure to execute the formal contract within the period of seven days specified by PIACL the Earnest money held by PIACL shall fortified and we / I shall not question the same.

Tenderer's Signature _____

Name in full_____
Designation _____
Address _____
_____
Phone /Fax# _____
CNIC _____
Seal _____
Date _____
Email Address _____