



31 AUG 2021

Journal of Management Research

## Services for Security Operations Center

THIS AGREEMENT is executed at KARACHI, on this day Sep 16 2021.

M/s Institute of Business Administration, through its Registrar, located at Main Campus, University Enclave, Karachi, hereinafter called and referred to as "IBA" (which expression shall wherever the context so permits, be deemed to include its legal representatives, executors, successors and assigns) of the FIRST PART.

M/s Supernet Limited, having its office at # 9<sup>th</sup> Floor, World Trade Center, 10 Khayaban-e-Roomi, Block 5, Clifton, Karachi, hereinafter referred to as "SERVICE PROVIDER" (which expression shall wherever the context so permits be deemed to include its legal representatives, executors, successor and assigns), through its presentative Mr. Sohail Hyder, holding CNIC No. 42201-1229025-5 on the SECOND PART.

**WHEREAS** "IBA" intends to obtain Services for Security Operations Center vide tender # IT/15/20-21 for the Services for Security Operations Center (IBA requirement) discussions in respect of the same before the determination of scope of supply will be held with "IBA" as "Services for Security Operations Center" and "THE SERVICE PROVIDER" have offered to render all kind of Services for Security Operations Center (including but not limited) to the "Services for Security Operations Center" of the proposed supply up to the satisfaction & handing over the material(s) to the "IBA" having accepted the offer in finished form complete in all respect.

NOW IT IS HEREBY AGREED & DECLARED BY AND BETWEEN THE PARTIES AS FOLLOWS:

WITNESSETH

"IBA" hereby offer to appoint "THE SERVICE PROVIDER" as their official for the specific purpose of "Services for Security Operations Center" discussions in respect of the same with "IBA" before the determination of Scope Services for Security Operations Center





with any/all other relevant details to "IBA". "THE SERVICE PROVIDER" hereby agrees to the offer of the "IBA" in acceptance of the terms & conditions here in below forth.

#### Article I

#### DUTIES & SCOPE OF SUPPLIES AND AGREEMENT

- 1.1 This Agreement includes, "Services for Security Operations Center", discussions with "IBA" before the determination of scope of supply with any/all other relevant details for presentation to "IBA".
- 1.2 "THE SERVICE PROVIDER" agrees to provide any/all kind of Services for Security Operations Center to "IBA" whenever and wherever form is required as per the terms & conditions of this Agreement.
- 1.3 "THE SERVICE PROVIDER" will coordinate with Head of Procurement, of the "IBA" who will assist "THE SERVICE PROVIDER" in supervision of proposed Services for Security Operations Center.
- 1.4 "THE SERVICE PROVIDER" hereby agrees to accept variation, if occurred, in scope of work deliverables as per tender vide # IT/15/20-21 with mutual consent on acceptable cost/price/charges/amount inclusive of all taxes and levies.
- 1.5 "THE SERVICE PROVIDER" will visit the Purchase Offices located at Main Campus, University Road, Karachi as & when required with prior appointment.
- 1.6 All logistic charges will be borne by "THE SERVICE PROVIDER".
- 1.7 The Institute of Business Administration (IBA) seeks the services of Security Operations Center (SOC) being managed, operated and maintained by third party service provider to enable IBA to prevent, detect, respond and recover from cyber security threats and events.
- 1.8 SIEM & SOC solution up to 100 Assets, including of Vulnerability Scanning, Log Ingestion, Threat feed, 24x7 SOC, Asset discovery.

#### Article II

#### SCOPE OF PROFESSIONAL SUPPLIES

- 2.1 "THE SERVICE PROVIDER" hereby agree and acknowledge for the periodic supervision of Services for Security Operations Center in accordance with the Description & Specification.
- 2.2 "THE SERVICE PROVIDER" hereby agrees and acknowledges the acceptance of attending the meetings with the Head of Procurement "IBA" as & when required.
- 2.3 "THE SERVICE PROVIDER", will provide all required/necessary transportation(s)/cartage(s) what so ever required to complete the procurement at the cost/charges amount offered in the tender vide # IT/15/20-21.
- 2.4 THE SERVICE PROVIDER should install the software and start delivering the satisfactory services within four weeks after signing of agreement.
- 2.5 SERVICE PROVIDER will ensure the following:

- (a) Preventive and corrective maintenance as recommended for the provisioned Software Appliance by Service provider, listed in this Agreement.





- (b) Physical inspection if required for virtual machine housing service provider installed Software Appliance/sensor
- (c) Periodic Performance tests and adjustments of Software Appliance/Sensors.
- (d) Performance engineering modification and changes, if recommended by IBA, and agreed by service provider, related to Service provider installed SIEM platform, Vulnerability scanning tool.
- (e) Virtual Appliance is fully operational and performs properly and meets SBD's (Standard Bidding Document) Requirements.
- (f) Responsible to respond to events\Incident on urgent basis as per SLA mention in this SBD.
- (g) Hardening IBA's environment for identify attack surface areas.
- (h) Review and analyze already established use cases for identification of any anomaly or incompleteness in-respect of threats and identified attack surface areas. Fine tuning and establishment of new use cases should be carried out where necessary.
- (i) Monitor and analyze the security event data to reveal / identify any anomaly or incident that can lead to jeopardizing availability, integrity and confidentiality of data.
- (j) Service provider should have robust threat intelligence mechanism that should be leveraged during detecting and remediating an incident.
- (k) Periodic reporting including daily tickets of events / incidents / attack(s) to the management and desired audiences as per agreed criteria.  
Service provider will also provide weekly/monthly Reports to relevant IBA team, with findings and remedial actions of the SIEM/Vulnerability platform.
- (l) In depth analysis of events/incidents with remediation guidelines.
- (m) On demand availability of historical event if required by IBA for forensic analysis.
- (n) Perform periodic table top blue team exercises to test the response and resilience level.
- (o) SOC services are required for 24 hours per day, 7 days a week and 365 days a year (24x7x365).

### Article III REMUNERATION

- 3.1 The cost offered by THE SERVICE PROVIDER is Rs. 5,984,550.00 (inclusive of all taxes) Services for Security Operations Center vide tender # IT/15/20-21 variation may have occurred. The cost is inclusive of labor/transportation/supplies/etc. Details of items are appended below;





S #	Platform Capabilities	Technical Details	Amount
1	Next Generation SIEM	NG-SIEM Services for servers and Workstation (Solution should be equipped with latest feature set like AI, Machine Learning (ML), Network Traffic Analytics (NTA) and User Behavior Analytics (UBA))	
		Flat per Asset Licensing (Not EPS, MPS/TPS, Log Volume based)	
		Cloud SIEM (O365/G-Suite/ AWS & Azure Active Directory)	
		Big data backend, Data Lake	
		Should have inbuilt Entity Behavior Analytics (EBA) capability	
		Should possess Network Detection and Response (NDR) with up to 1Gbps Traffic Ingestion	
		Should be an XDR based platform	
		Cyber Kill Chain mapping with detection playbooks (New detections should be added continuously by the solution provider)	
		Integrated Threat Intelligence	
		Correlation Engine	
		AI/Machine Learning for anomaly detections	
		Log enrichment, Drill Down, Threat Context of Alerts	
		Threat Hunting Module	
		Agents Sensor for Windows, Linux, VMware, Containers, Hyper-V	
		Syslog forwarding	
		Asset discovery (Approved vs Unapproved Assets detections)	
		Services Discovery and Analytics	
		Applications and Protocol Discovery and Analytics	
		Network deep packet inspection	
		One Year full log retention	
		Support Off-Site log Archiving and should be part of solution with no additional cost	
2	Vulnerability Management	The Solution Should be a specialized solution of VA, and have presence in Gartner Magic Quadrant, rather than any simple built-in module.	
		Vulnerability Risk Scoring	
		Active, Passive scanning with real-time visibility of environment changes	
		Policy Assessment (e.g. NIST, CIS)	
		Remediation Reports	
		NIST Vulnerability Database	
		Asset Compliance Dashboard (SCAP)	
3	Environment Hardening during Installation Phase	The solution must have Minimum 30 Days	
		Handholding/Consultancy as part of proposed solution	
		IBA Environment Hardening (Help reducing attack surface), based on the guidelines of NIST Cybersecurity Framework (NIST-800)	



		Assurance of CIS Top 20 Controls Mapping (Reduces Risks) before handing over	
		Project Supervision by at least CISSP Certified consultant	
		Use case Development relevant to IBA	
		SIEM Integration, Data point identification	
		Best Practice Recommendations and Anomalies correction guidelines	
		Vulnerability Management System Deployment	
4	SOC Monitoring Services	Solution should have Tiered SOC Monitoring (Global SOC + Regional SOC)	
		24x7x365 SOC threat, event and incident alerting	
		24x7x365 SOC analysis, recommendations, and escalations	
		Vulnerability Remediation Assistance	
		Pervasive Security Visibility via Real-time Dashboards	
		Scheduled vulnerability scanning	
		Weekly vulnerability reporting vetted by Security Experts	
		On-demand Custom Reports	
		CIS20 SOC reports, should be provided on monthly basis	
5	SOC Procedures & Policies	The solution should be based on NIST Cybersecurity Framework (NIST-800)	
<b>Total (Per Year)</b>			Rs. 5,115,000.00
<b>17%</b>			Rs. 869,550.00
<b>Grand Total Amount</b>			Rs. 5,984,550.00

### 3.2 Liquidity damages:

- (a) In case of breach of SLA, calculation will be done as per table below and IBA reserves the right to impose a penalty not exceeding 10% of the total amount of the contract at the rates prescribed on the invoiced amount to each violation of SLA.
- (b) If Service provider does not carry the agreed scope of work properly, IBA can issue warning, deadline to remediate the work.  
Service provider will be held liable to execute the agreed scope of work only, any scope creep, additional requirement, (other than this Agreement scope) would not apply on service provider to execute.

If condition reaches to a point where one party tends to not continue, the decision will be made with mutual consent, referring to termination clause as defined below in the Agreement.

Both parties will work in conjunction to avoid reaching at this point.

- (c) In case of delay in service provisioning Liquidated Damages will be Calculated and imposed as per following table





### 3 Levels

Level	Event	% of Invoiced amount per violation
L1	High	1%
L2	Medium	0.5%
L3	Low	0.3%

- 3.3 Performance Security 5% of total amount of Purchase Order will be provided by the party.
- 3.4 Stamp Duty @ 0.35% of the cost of transaction / purchase order will be deposited in Government treasury by THE SERVICE PROVIDER. This paid Stamp Duty challan would be submitted along with the Bill / Invoice.
- 3.5 Tax(es)/Challan(s)/Levy(ies), Custom Duty/Excise Duty etc. if any or additional will be paid/borne by SUPPLIER as per SRO/Notification.

#### Article IV

#### ANNUAL SUPPORT & MAINTENANCE TERMS

- 4.1 The Annual Support and Maintenance of the SLA for Services for Security Operations Center shall include the following activities
- One (1) year maintenance support with all Services for Security Operations Center listed above.
  - M/s Supernet Limited will be required to undertake Support and Maintenance for the SLA for Services for Security Operations Center and related components as follows:
  - Quarterly onsite perform vulnerability assessment of all 100 assets include the following:
    - Environment Hardening based on the guidelines of NIST Cybersecurity Framework (NIST-800)
    - Assurance of CIS Top 20 Controls mapping (Reduces Risks) during the exercise of Network hardening.
    - Service provider will be responsible of vulnerability remediation assistance to IBA Network Operation team.
    - Provide pervasive Security Visibility via Real-time Dashboards.
    - Vulnerability Risk Scoring and Policy assessment.

#### Article V

#### SLA TIME MATRIX

- 5.1 THE SERVICE PROVIDER shall provide the required services as per SLA matrix given below: -

Ticket Type	Severity	Escalation 1	Escalation 2	Escalation 3	Escalation 4	SLA
Security Incident	High	Supernet provided 24x7 alert response email address (Within 30 Mins)	Supernet SOC Technical Contact** (After 45 Mins)	Supernet Manager/Team Lead SOC (After 60 Mins)	Supernet Head of Technology (CTO) / CEO (After 90 Mins)	Within 30 Minutes





Security Alert	Medium	Supernet provided 24x7 alert response email address (After 60 Mins)	Supernet's SOC Primary Contact* (After 90 Mins)	Supernet SOC Technical Contact (After 120 Mins)	Supernet Manager/Team Lead SOC (After 180 Mins)	Within 60 Minutes
Security Event	Low	Supernet provided 24x7 alert response email address (Within 12 hours)	Supernet provided 24x7 alert response email address with reminder (After 14 hours)	Supernet's SOC Primary Contact* (After 16 Hours)	Supernet SOC Technical Contact & Account Manager (After 24 hours)	Within 24 hours max

\*Supernet SOC Primary Contact: Where customer can reach to 24x7 SOC team directly in getting remediation guidelines

\*\*Supernet SOC Technical Contact: Where customer can reach to an assigned security Engineer directly via email or call.

Definitions:

- An **event** is an observed change to the normal behaviour of a system, environment, process, workflow or person. *Examples: usage anomalies, Authentication anomalies, network anomalies, suspicious process, non-business hours activities, communication with known malicious external host, identified vulnerabilities, gaps.*
- An **alert** is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action. *Examples: the events above sent to client designated emails, on-call personnel.*
- An **incident** is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business. *Examples: system compromised, worm spreads through network, successful exploitation.*

We adhere to the following Standard Service Level Agreement via the below escalation processes on a best endeavours basis.

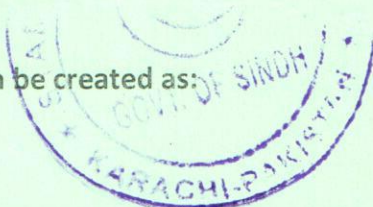
Generally speaking, all requests outside of standard deployment steps will require a ticket to be created. This will ensure requests are properly tracked and visible to all SOC team members and leadership to best support you.

Definitions

**Incident Handler:** The identified email address or distribution list that is typically associated with a client in which the SOC will send tickets to for incident communications to the client.

**Inbound Ticket:** Request initiated into the SOC, not related to a specific incident, requiring response from the SOC. These typically include report requests, deployment questions, user interface knowledge transfer and other general inquiries from client.

Tickets can be created as:





1. Customer can email **soc-irt@Supernet.pk** to generate a ticket from a previously authorized email domain.
2. Customer can call at our Primary # XXXX

Clients requiring that their ticket to be escalated can email their ticket number to **soc-irt@Supernet.pk**.

Inbound tickets will be supported according to the service level agreement as outlined within the client contract for devices and sites outlined within this agreement. This will be determined at the point of sale. List will be added as an Annexure, after finalization of the Assets between client and Supernet.

*\*\*SLAs do not apply for remediation work and are adhered to on a best endeavors basis.*

• **Security Threat: EXAMPLE**

o Office 365 Login Failure from China *(Just an Example)*

- Detect | CSC 16 | Sub control 16.12
- Full Hits: 50
- Tenant Name
- Timestamp 2020-01-06T20:39:58.834Z
- Application Name o365\_login
- Source Host 58.1.1.4
- Source IP 58.1.1.4
- Source City Chongqing
- Source Country China
- Source IP Reputation Good
- Destination Host
- Destination IP
- Destination City
- Destination Country
- Destination IP Reputation
- Event Category
- Username xxxxxx.xxxxx@abc.com
- Login Result fail

• **Security Event: EXAMPLE – Successfully Established WAN to LAN Remote Desktop Session**

o Remote Desktop Access Detected from WAN to LAN

- Category: Detect | CSC 9 | Sub-control 9.11
- Full Hits: 4
- Tenant ID 12345678
- Detection Date
- Detection Time
- 11
- Source Host srv38.malwareserver.net
- Source IP 1.2.3.4
- Source City Moscow



- Source Country Russian Federation
- Destination Host 10.0.1.10
- Destination IP 10.0.1.10
- Destination City Los Angeles
- Destination Country United States
- Session State Established

#### Responsibilities Matrix

- Client must supply (and not unreasonably withhold) important or accurate information at the outset or when requested subsequently by us while investigating a security alert.
- Client (and any related third party) must respond to or act upon our reasonable instructions and/or requests for assistance in a timely manner.
- Both parties will monitor and review SLA performance on an ongoing basis.
- We will not be deemed to be in breach of the SLA in the event that a crucial element of the relevant monitored network (and/or detection points) is/are not available to us to permit us to provide the Services, including (but not limited) to availability of your network and/or internet connectivity or in any other circumstances outside of our control such as (but not limited to) any circumstance that would amount to a Force Majeure Event.

#### Article VI DATA PROTECTION

6.1 In addition to and notwithstanding any other right or obligation arising under this Agreement the SERVICE PROVIDER shall (and shall ensure that its sub-contractors shall) take all appropriate technical and organizational security measures to ensure that any or all Data is protected against loss, destruction and damage, and against unauthorized access, use, modification, disclosure or other misuse, and that only the SERVICE PROVIDER personnel designated for the purpose of Services have access to the Data.

6.2 The SERVICE PROVIDER shall (and shall ensure that its employees, agents and subcontractors shall) in respect of the Data:

- (a) comply with any request made or direction given by IBA in connection with the requirements of any Data Protection Laws; and not do or permit anything to be done which might jeopardize or contravene the terms of any registration, notification or authorization under the Data Protection Laws; and not process any Data (including personal or private information of personnel, employees of IBA, as part of the Services unless it is acting on the express written instructions of IBA, and such Data shall be treated as Confidential Information of IBA for the purpose of this Agreement; and
- (b) use the Data only for the purposes of fulfilling its obligations under this Agreement and to comply with instructions of IBA from time to time in connection with use of such Data, and not retain the Data for any longer than is necessary for these purposes; and
- (c) not disclose the Data without the written authority of IBA (except for the purposes of fulfilling its obligations under this Agreement), and immediately notify such member where it becomes aware that a disclosure of Data may be required by law; and not transfer Data which has been obtained by or made available to the SERVICE PROVIDER within one country outside that country, or allow persons outside that country to have access to it, without the prior written approval of IBA; and



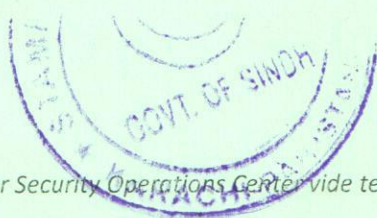
- (d) observe the provisions of, and comply with any request made or direction given by IBA in connection with, any Data Protection Laws; and
- (e) take all reasonable steps to ensure the reliability of the personnel which will have access to any Data and ensure that any employee of the SERVICE PROVIDER (or of any of the SERVICE PROVIDER's sub-contractors) requiring access to any Data gives a written undertaking not to .A; access, use, disclose or retain the Data except in performing their duties of '}) employment and is informed that failure to comply with this undertaking may be a criminal offence and may also lead the SERVICE PROVIDER (or, as the case may be, sub-contractor) to take disciplinary action against the employee; and
- (f) consider all suggestions by IBA's personnel to ensure that the level of protection provided for the Data is in accordance with this Agreement and to make the changes suggested (at the SERVICE PROVIDER's cost) unless the SERVICE PROVIDER can prove to IBA's reasonable satisfaction that they are not necessary or desirable to ensure ongoing compliance with this Clause;
- (g) Immediately notify IBA when it becomes aware of a breach of this Clause.
- (h) The SERVICE PROVIDER acknowledges that any unauthorized access, destruction, alteration, addition or impediment to access or use of that Data when stored in any computer, or the publication or communication of any part or document by a person which has come to his knowledge or into his possession or custody by virtue of the performance of this Agreement (other than to a person to whom the SERVICE PROVIDER is authorized to publish or disclose the fact or document) may be a criminal offence.

#### Article VII ADD-ON-Virtual Appliance

6.3 As per the tender IT/15/20-21, scope of the project is limited to delivery of Software Appliance of SIEM and Vulnerability management tools and 24x7x365 SOC support. The software Appliance has the capacity of 100 Assets and 02 sensors. Anything beyond to that, if required technically will be qualified by both parties and will be made part of the solution/agreement at the agreed new cost.

#### Article IX SERVICES / OBLIGATIONS OF THE SERVICE PROVIDER

- 9.1 The following section provides a detailed list of the Standard Services that are to be delivered to the Client under the terms of this Agreement.
- 9.2 The prime deliverables of the Service provider are the Software Appliance for SIEM and Vulnerability management tool, it is hereby specifically agreed between the Parties that during the currency of this Agreement, and any renewal thereof, Service Provider shall be responsible for patch/version up gradation, OS Update/upgrade of the provisioned software Appliance, remediation of any corrupted file. The VM ware/ any hardware provided by IBA will remain in the supervision and maintenance of IBA.





**Article X**  
**ESCALATION MATRIX**

**Hours of Coverage**

The Service Provider will provide maintenance and support for 24x7 Basis.

**Response Time**

Response time to incidents reported would be as follows:

Severity Level	Response Time
Severity Level 1 (High)	30 minutes
Severity Level 2 (Medium)	1 hour
Severity Level 3 (Low)	Within 24 hours

**Article XI**  
**ARBITRATION**

11.1 In case of any dispute, difference or and question which may at any time arise between the parties hereto or any person under them, arising out in respect of this letter of intent or this subject matter thereof shall be referred to the Registrar of the IBA and CEO of the company / firm / agency for arbitration/settling of the dispute, failing which the decision of the court law in the jurisdiction of Karachi binding to the parties. The Arbitration proceedings will be governed by the Arbitration Act, 1940 and the Substantive and procedural law of Pakistan. The venue shall be Karachi.

**Article XII**  
**TERMINATION**

- 12.1 Term. The term of this Agreement shall commence upon the Effective Date (effective date is the date on which SOC and SIEM services will be activated and informed to IBA) and remain in effect for the period of ONE YEAR, unless earlier terminated as set forth herein. The Term shall be for a period of one (1) year from effective date.
- 12.2 Either party can terminate this Agreement by giving written notice to terminate at least six (6) months prior to the expiry of the Term or the relevant extension period as the case may be. In addition to amounts owing to the date of termination pursuant to this Agreement, the remaining term of each IBA-Service Provider 's contract shall remain payable until expiration or termination.
- 12.3 Either party may terminate this Agreement, upon written notice for any material breach of this Agreement to the other party and failure to cure within thirty (30) days following written notice specifying such breach. For avoidance of doubt, IBA's failure to pay invoice amounts under this Agreement shall constitute a breach of this Agreement. Upon expiration or termination of this Agreement, Customer will cease all use of the software appliance.
- 12.4 Subject to clause 12.1, 12.2 and 12.3, each party acknowledges that in the event of termination of this Agreement pursuant to its terms, it shall have no right to damages or indemnification of any nature resulting from such termination, whether by way of loss of goodwill, future profits, or revenue, on account of expenditures



investments, or other commitments in connection with its business or goodwill or otherwise.

Article XIII  
INDEMNITY

13.1 "THE SERVICE PROVIDER" in its individual capacity shall indemnify and keep IBA and any person claiming through IBA fully indemnified and harmless from and against all damages, cost and expenses caused to or incurred by "THE SERVICE PROVIDER", as a result of any defect in the title of IBA or any fault, neglect or omission by the "THE SERVICE PROVIDER" which disturbs or damage the reputation, quality or the standard of services provided by "IBA" and any person claiming through the IBA.

Article XIV  
NOTICE

14.1 Any notice given under this AGREEMENT shall be sufficient if it is in writing and if sent by courier or registered mail.

Article XV  
INTEGRITY PACT

- 15.1 The intention not to obtain the procurement / purchase of any Contract, right, interest, privilege, or other obligation or benefit from the IBA or any administrative or financial offices thereof or any other department under the control of the IBA through any corrupt practice(s).
- 15.2 Without limiting the generality of the forgoing the M/s Supernet Limited, represents and warrants that it has fully declared the charges, fees, commission, taxes, levies etc., paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within the IBA directly or indirectly through any means any commission, gratification, bribe, gifts, kickback whether described as consultation fee or otherwise, with the object of obtaining or including the procurement or service contract or order or other obligations whatsoever from the IBA, except that which has been expressly declared pursuant hereto.
- 15.3 M/s Supernet Limited accepts full responsibility and strict liability for making any false declaration/statement, not making full disclosure, misrepresenting facts or taking any action likely to degrade the purpose of declaration, representation and warranty. It agrees that any contract/order obtained aforesaid shall without prejudice to any other right & remedies available to the IBA under any law, contract, or other instrument, be stand void at the discretion of the IBA.
- 15.4 Notwithstanding any right and remedies exercised by the IBA in this regard, M/s Supernet Limited, agrees to indemnify the IBA for any loss or damage incurred by it on account of its corrupt business practice & further pay compensation to the IBA in any amount equivalent to the loss of any commission, gratification, bribe, gifts, kickback



given by the M/s Supernet Limited, as aforesaid for the purpose of obtaining or inducing procurement or other obligation or benefit in whatsoever from the IBA.

**Article XVI**  
**SEVERABILITY**

16.1 If any terms covenant or condition of this agreement shall be deemed invalid or unenforceable in a court of law or equity, the remainder of this agreement shall be valid & enforced to the fullest extent permitted by prevailing law.

**Article XVII**  
**PAYMENT**

17.1 Payment shall be released at the end of each quarter after submission of commercial invoice.

**Article XVIII**  
**RENEWAL**

18.1 This Agreement shall be renewed with mutual consent & satisfactory performance upon completion of one year if the IBA, Karachi and the SERVICE PROVIDER agree so.

18.2 Extension Period. Notwithstanding the foregoing, if the Term of this agreement is required to be extended beyond the Term of this Agreement ("Extension Period"), this Agreement shall will be required to extend for a minimum of ONE YEAR.

18.3 All other terms of this agreement will remain same and commercial terms will be required to agree for the extension period.

18.4 Notice for extension will be required from IBA to Service provider at least 30 Days from the expiry of the term.

**Article XIX**  
**MISCELLANEOUS**

19.1 Any addition & alteration(s) made for work deliverables as required by IBA on the basis of proof of Concept or in course of the work-in progress which entail extra time & labor and material on part of the supply, shall not be charged separately/extra on 'Quantum Merit' basis before & on final material handed over to the "IBA". After FINALIZATION OF proof of concept, if any alteration(s), arise charges will be paid on mutually agreed upon.

19.2 Service delivery handing over, as per Tender vide # IT/15/20-21 scope, to IBA or vetting of any cost by Service provider or IBA should be closed with authentic stamp and signature of both parties.


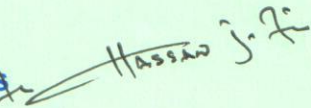
19.3 The terms and conditions of the AGREEMENT have been read over to the parties which they admit to be correct and abide by the same.

19.4 The validity of the contract will be effective from the date of issue of Purchase Order.

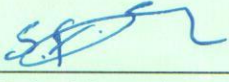
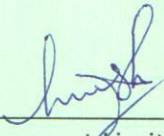


19.5 All terms and conditions of tender vide # IT/15/20-21 will be the integral part of this agreement and can't be revoked.

IN WITNESS WHEREOF both the parties hereto have set & subscribed their respective hands to this agreement at Karachi on the date as mentioned above.

 <b>Dr. Muhammad Asad Ilyas</b> Registrar Former Chairperson Accounting & Law Department Institute of Business Administration (IBA) Karachi, Pakistan "IBA" NAME: Dr. Muhammad Asad Ilyas CNIC # _____ Address: <u>Registrar, Institute of Business</u> <u>Administration Main Campus</u> <u>University Enclave, Karachi</u>	 NAME: <u>HASSAN SABIR</u> CNIC # <u>42101-3171707-7</u> Address: <u>9<sup>th</sup> Floor, World Trade Center</u> <u>10 Khayaban-e-Roomi Block 5, Clifton</u> Karachi
---	---

**WITNESS:**

<p>1.  Syed Fahad Jawed CNIC # <u>42201-9125136-3</u> Address: <u>Head of Procurement</u> <u>Institute of Business</u> <u>Administration Main Campus</u> <u>University Enclave, Karachi</u></p>	<p>2.  M/s Supernet Limited NAME: <u>Sohail Hyder</u> CNIC # <u>42201-1229025-5</u> Address:</p>
--	--

Focal Person IBA

Wajeeh Zaidi

