NOTICE OF REQUEST FOR QUOTATION (RFQ)

Vendors are invited from company incorporated in Malaysia and registered with Tenaga Nasional Berhad (TNB) for supply, installation and commissioning of work as follows:

RFQ Description	OPEN RFQ FOR SUPPLY, DEPLOYMENT AND MAINTENANCE OF DISTRIBUTED DENIAL-OF SERVICE ("DDOS") DETECTION, MITIGATION AND TRAFFIC SCRUBBING SOLUTION FOR ALLO TECHNOLOGY SDN. BHD.
Category of Works/Supplies	Network
RFQ Floatation Date	Tuesday, 28th April 2026
RFQ Closing Date	Tuesday, 12th May 2026 (12.00 Noon)
Submission of RFQ Documents	The RFQ Documents shall be submitted in **hardcopy.** *(optional - softcopy via USB Drive)* **Please attached together the SSM and/or TNB vendor registration certificate*
Submission of the RFQ Documents shall be hand delivered to Allo Tender Box as per the following address:	ALLO TECHNOLOGY SDN BHD Level 3, Left Wing, NOVA Building, Universiti Tenaga Nasional (UNITEN), 43000 Kajang, Selangor. (Attn: Procurement & Supply Chain Department) (**RFQ No: ALLO-RFQ-DDOS-2026**)

1. **Qualification/Mandatory Requirement**

   - A company is legitimate and incorporated in Malaysia and has been duly registered with Companies Commission of Malaysia (SSM) and/or Registered as a vendor with Tenaga Nasional Berhad (TNB).

2. **Contact info for Technical Enquiries**
   - Contact Person: Juhaimi Nizam Johari
     Email: juhaimi@allo.my
   - Contact Person: Mohd Zamri Mohd Salleh
     Email: zamri@allo.my

3. **Contact info for RFQ General Enquiries**
   - Contact Person: Muhammad Qayyum Mohd Nor
   - Email: qayyum@allo.my / procurementallo@allo.my

NOTICE OF REQUEST FOR QUOTATION (RFQ)

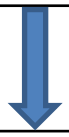
4. Submission of RFQ Document

Flow process for RFQ documents submission as per below:

SINGLE MASTER ENVELOPE / SINGLE PARCEL PACKAGE

What to do:

1. Include the RFQ documents into a **SINGLE MASTER ENVELOPE** OR **SINGLE PARCEL PACKAGE.**
2. Submission shall be in **SEALED** Single Master Envelope or Single Parcel Package and placed in Allo's Tender Box.
3. Affix label as shown below



HAND-DELIVERY TO:

Allo Technology Sdn Bhd,
Level 3, Left Wing,
NOVA Building, Universiti Tenaga Nasional (UNITEN),
43000 Kajang, Selangor.

(Attn: Procurement & Supply Chain Department)
(RFQ No: ALLO-RFQ-DDOS-2026)

No later than 12.00 Noon on Tuesday, 12th May 2026

ALLO TECHNOLOGY SDN BHD
PROCUREMENT UNIT

Appendix A
RFQ: SUPPLY, DEPLOYMENT AND MAINTENANCE OF DISTRIBUTED DENIAL-OF SERVICE ("DDOS") DETECTION, MITIGATION AND TRAFFIC SCRUBBING SOLUTION FOR ALLO TECHNOLOGY SDN. BHD.

			1 YEAR CONTRACT					2 YEARS CONTRACT					3 YEARS CONTRACT				
			OUTRIGHT PURCHASE			LEASE TO OWN		OUTRIGHT PURCHASE			LEASE TO OWN		OUTRIGHT PURCHASE			LEASE TO OWN	
No.	Description	U.O.M.	Quantity	Price/Unit	Total (RM)	Price/Unit	Total (RM)	Quantity	Price/Unit	Total (RM)	Price/Unit	Total (RM)	Quantity	Price/Unit	Total (RM)	Price/Unit	Total (RM)
1	**DISTRIBUTED DENIAL-OF SERVICE ("DDoS")** - On Premise solution (Hardware+Support+Managed DDOS Services)																
1.1	**HARDWARE:** **with NBD hardware maintenance*	Unit	1		-		-	1		-		-	1		-		-
1.2	**NETWORK PROTECTION LICENSE - 10 GBPS (LAYER 3/4 PROTECTION)** Site License for use with: - Server with 10GBPS Mitigation Throughput. - License includes 100 Configurable Site Security Profiles. - No flows per second licenses and no protected routers included. Flow Monitoring License for receiving and processing flow telemetry from customer networks for 1,000 flows per second (fps). 3x Licenses for 1 connected routers to be monitored/protected.	Set	1		-		-	1		-		-	1		-		-
1.3	**MANAGED ANALYST SERVICES** - Including threat triage, incident investigation, traffic forensics, service provisioning, policy advisory, technical enablement, participation in client meetings, and escalation to Tier 2-3 support engineers.	Year	1				-	2		-		-	3		-		-
1.4	**ONE TIME SETUP FEE**	Lot	1		-		-	1		-		-	1		-		-
	Compulsory Requirements: *Tenderers are required to comply with the Technical Compliance requirements set out in ***Section I – Provision for Service of Compliance ("SOC") and Scope of Works ("SoW").*** **Site Location :** MY01 Data Center, Cyberjaya																
SST (RM)																	
GRAND TOTAL PRICE INCLUSIVE OF ALL APPLICABLE TAXES (RM)					-		-			-		-			-		-

SERVICE COMPLIANCE AND SCOPE OF WORKS
1) As per Section I – Provision for Service of Compliance ("SOC") and Scope of Works ("SoW").
kindly ensure that the company stamp is affixed on every page and that the document is duly signed on the last page.

Compliance	
Payment Term : 45 days upon document verification and acceptance by Allo. (refer Appendix of POTC for milestone payment term). - Other terms please refer the POTC and the Appendix. - Insurance - Refer POTC	Yes/No
Completion date: Two (2) months upon PO issuance	Yes/No

I acknowledge that I have read, understand and comply to the above job description in its entirety and capable of performing all of the stated requirements:

Company Name:
Name:
Email:
Phone No:
Company stamp:
Date:

SECTION I PROVISION FOR STATEMENT OF COMPLIANCE (“SOC”) AND SCOPE OF WORKS (“SoW”)

Background

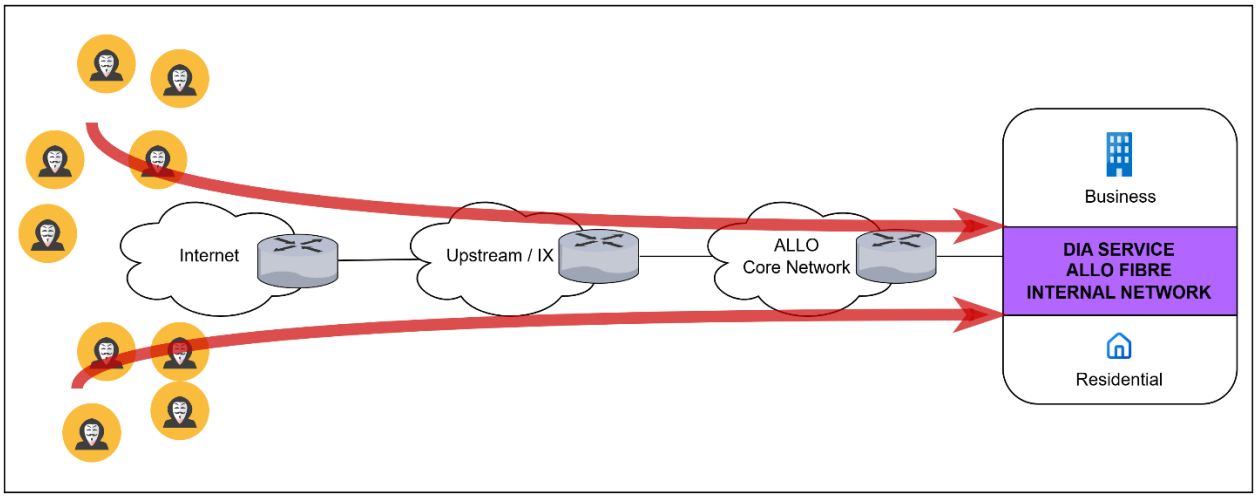


Figure 1: Without DDoS Protection – Attacks directly impact Allo services and customers.

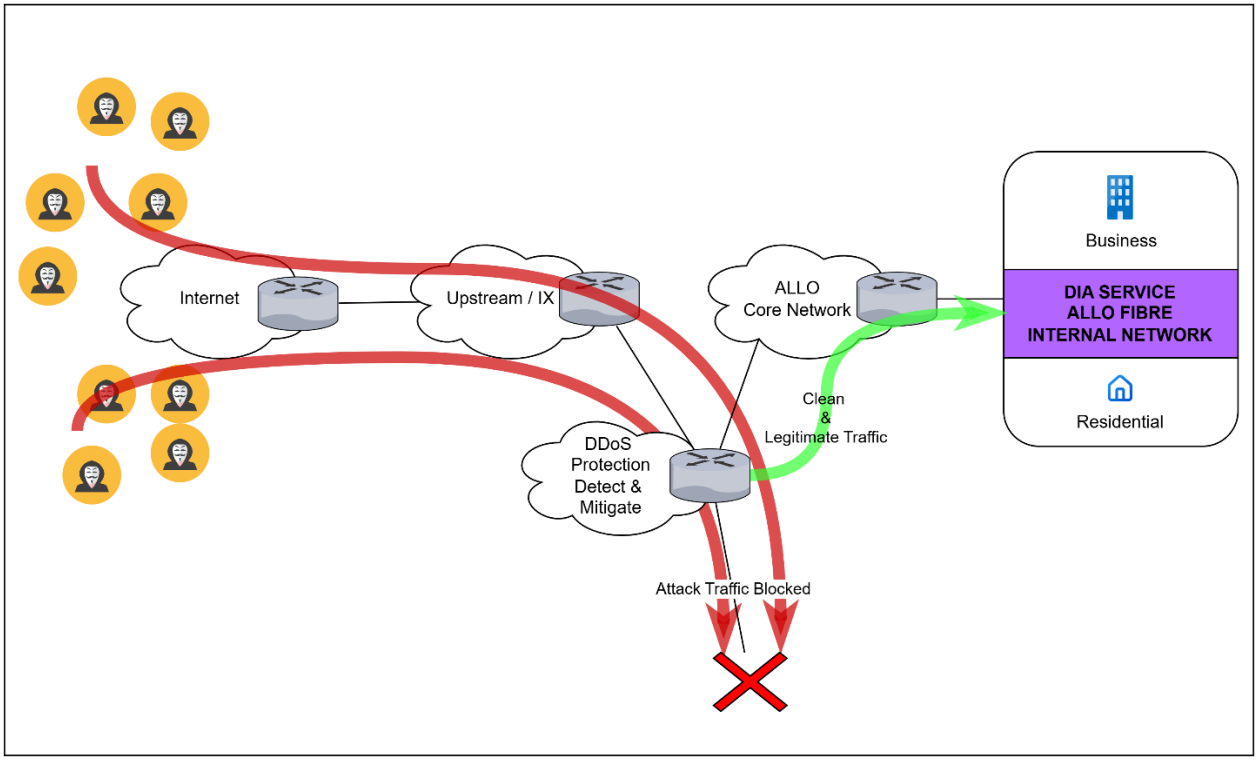


Figure 2: With DDoS Protection – Attacks are mitigated before entering Allo's network.

Statement of Compliance (SoC) & Scope of Work (SoW)

CRQ - Critical Requirement Critical requirements are the most important requirements regarding the functionality of the solution or the qualification of the Vendor and are essential for the proper functioning of the target network and a future proof development path. Compliance is a must and no alternatives are permitted. Non-compliant to a CRQ of the tender can result in exclusion from further evaluation.
MRQ - Major Requirement These requirements are important for the functionality of the building blocks or components of the solution and therefore will be treated with high priority. The Vendor must provide a response for each MRQ requirement in the compliance list.
REQ - Normal Requirement These requirements are requested to meet certain functionalities depending on the methods and approach to be utilized by the Vendor. The Vendor must provide a response for each REQ requirement in the compliance list.
IRQ - Information Request The Vendor is required to explain and describe their own approach or methodology for this purpose. For each IRQ, the supporting document(s) must be provided with file name that corresponds to the requirement ID number.

2.0 Scope of Works ("SoW")

Scope of Work

No.	General Technical Specification for Managed DDoS Detection and Mitigation System	Category
a	The solutions must allow Allo to build scrubbing in their own network	CRQ
b	The solution should support Cloud Offload should the DDoS attack exceeds the network / scrubbing capacity. The activation of the feature shall be fully automated without manual interaction.	CRQ
c	The solution should consist of DDoS Detector, Mitigator and Management device On-premises and Cloud Offload.	CRQ
d	The solution shall support BGP and out of path deployment.	CRQ
e	The solution should be designed to ensure high availability and service continuity, with no disruption to operations in the event of any system or hardware failure.	MRQ
f	The proposed Managed DDoS Detection and Mitigation System shall have proven and certified deployments in at least five (5) Internet Service Provider (ISP) environments within the past three (3) years.	MRQ
g	The proposed Managed DDoS Detection and Mitigation System must have received recognized industry acknowledgment within the last three (3) years as a leading or top-rated provider in an independent third-party evaluation report (e.g., SPARK Matrix, Gartner, Frost & Sullivan) for DDoS Mitigation Solutions.	MRQ
1.0	Detection & flow collection	
1.1	The system should monitor IP traffic of multiple class Cs / variable IP prefix length.	CRQ
1.2	The system should support at least 1,000 class C IP addresses.	MRQ
1.3	Each system shall support at least 50k flow per second (fps).	MRQ
1.4	The system shall support the following flow protocols: - Netflow v5 / 9 - IPFIX - sflow v2 / 4 / 5 - Netstream v5 / 8 / 9	MRQ
1.5	The system should generate email alerts if flow data is not received within a pre-configured time window.	CRQ
1.6	The system shall be able to poll under monitor routers using SNMP v2c.	MRQ
1.7	The system shall be able to detect bandwidth depletion attacks including but not limited to the following: - TCP floods - SYN, ACK, RST, Null - UDP floods - DNS flood - ICMP floods - Smurf, ping flood, Ping of Death, ICMP echo - Spoofed-packet floods - Fragmentation - IP/UDP, IP/ICMP, IP/TCP, Teardrop - Amplification - DNS, NTP, SNMP, SSDP, CHARGEN, L2TP, MDNS, MS SQL RS, NETBIOS, RIPv1, RPCBIND, MEMCACHED - IP Bogons, LAND attacks - SIP flood	MRQ

1.8	The system shall support AI-based flood detection.	MRQ
1.9	The system shall support multiple level CIDR based on a managed object detection policy. This allows SOC to define a common set of detection thresholds on the SITE level while allowing customized thresholds suiting individual /24 networks or /32 hosts.	CRQ
1.10	The system shall detail all DDoS events on the customer / admin portal with the following info: - start time of the attack - size of the attack in bps & pps - duration of the attack - status of the attack - under attack IP address and service ports - attack type - top 100 traffic patterns - packet size distribution - threat map - IP of router detecting attack - traffic graph during the DDoS event	MRQ
1.11	The system shall allow customer portal users to tag the event as: - DDoS attack - Not DDoS attack - Uncertain	CRQ
1.12	The system shall detect application-layer (Layer 7) DDoS attacks including but not limited to HTTP GET/POST floods, slow HTTP attacks (Slowloris), TLS/SSL handshake exhaustion, and malformed application requests.	MRQ
1.13	The system shall support configurable traffic baseline learning periods per managed object to establish normal traffic behavior prior to enforcement of detection and mitigation policies.	MRQ
1.14	The system shall allow immediate manual override, rollback, or termination of mitigation actions in the event of false positive detection without service disruption.	CRQ
2.0	Mitigation	
2.1	The DDOS mitigation system shall support at least 3Tbps mitigation capacity	MRQ
2.2	The mitigation system shall be able to mitigate multi-vector DDoS attacks.	CRQ
2.3	The mitigation system should support auto-mitigation.	CRQ
2.4	The mitigation system shall provide anti-flooding policy against - TCP floods - SYN, ACK, RST, Null - UDP floods - DNS flood - ICMP floods - Smurf, ping flood, Ping of Death, ICMP echo - Spoofed-packet floods	MRQ
2.5	The mitigation system shall support zombie filters to detect as well as rate limit or drop traffic sent from compromised host.	MRQ
2.6	The mitigation system shall support traffic policing to shape the traffic	MRQ

	delivered to the destination network / host.	
2.7	The mitigation system shall support traffic blackholing as last line of defense.	MRQ
2.8	The proposed Equipment shall be able to support IPv4 & IPv6 BGP routing protocols for traffic mitigation.	MRQ
2.9	The proposed mitigation device should provide packet capture function during DDoS mitigation.	MRQ
2.10	The proposed system must be able to advertise the IPv4 /32 or IPv6 /128 prefix mitigation route to Border router by using the eBGP peering session.	CRQ
2.11	The proposed system must be able to redistribute the /32 or /128 mitigation route prefix to Border Router via iBGP peering session.	CRQ
2.12	The mitigation system shall support stateful traffic analysis to differentiate legitimate traffic from attack traffic during volumetric, reflection, and multi-vector DDoS attacks.	MRQ
2.13	The mitigation system shall ensure that the additional latency introduced to clean traffic during mitigation does not exceed predefined acceptable limits within the same geographic region.	CRQ
2.14	The mitigation system shall support static and dynamic whitelisting and blacklisting of IP addresses, IP prefixes, protocols, and service ports during mitigation.	CRQ
3.0	Alerts including DDoS attack alerts	
3.1	The system will be able to notify registered portal users' email addresses on DDoS attack alert.	CRQ
3.2	The system shall be able to notify registered portal users' email addresses if no flow data is received for a pre-defined period.	CRQ
3.3	The system shall be able to notify registered portal users' email addresses on route changes.	CRQ
3.4	The system shall notify the 24x7 Security Operations Center (SOC) automatically upon detection of DDoS attacks and mitigation events, including escalation for high-severity incidents.	CRQ
4.0	Traffic diversion	
4.1	The system shall be able to receive BGP route advertisement from BGP peer routers.	CRQ
4.2	The system shall be able to establish GRE tunnel with customer's router.	CRQ
4.3	The system shall be able to re-inject clean traffic via multiple GRE tunnels established.	MRQ
4.4	The system shall be able to support at least 1,000 established GRE tunnels.	MRQ
4.5	The system shall support multiple VLANs to segregate raw traffic, mitigate traffic and clean traffic.	MRQ
4.6	The system shall be able to inject BGP routes into the network to divert under attack IP prefix to itself to mitigate the attack.	CRQ
4.7	The system shall support asymmetrical traffic path.	MRQ
4.8	The system shall support automatic traffic diversion on activation of global offload.	CRQ

4.9	The system shall support diversion of dirty traffic from Border Router	MRQ
4.10	The system shall support the clean traffic to be reinjected back to Border router after mitigation.	MRQ
4.11	The system shall support Border router to send the clean traffic back to customer network.	MRQ
4.12	The cloud-based DDoS scrubbing centers shall be located within the Asia-Pacific or ASEAN region to minimize latency impact on customer traffic.	CRQ
4.13	The system shall automatically revert diverted traffic back to on-premises mitigation or normal routing once the DDoS attack has subsided without manual intervention.	CRQ
4.14	The bidder shall declare the total available cloud-based DDoS mitigation capacity and per-site scrubbing capacity as part of the proposal.	MRQ
5.0	Management portal	
5.1	The admin portal access shall support secure HTTPS access only.	CRQ
5.2	The admin portal shall support role base access control policy. This policy defines the access privilege and the authorized action allowed for both the admin / customer portal user.	CRQ
5.3	The admin portal shall support standard web browsers such as Chrome & Firefox.	REQ
5.4	The admin portal shall provide a centralized view of all the customers' profiles under protection.	CRQ
5.5	The Admin portal shall provide a centralized view of all live and ongoing DDoS events for the under protection customers' profile with detail including but not limited to - start time of the attack - size of the attack in bps & pps - duration of the attack - status of the attack - under attack IP address and service ports - attack type - top 100 traffic patterns - packet size distribution - threat map - IP of router detecting attack - traffic graph during the DDoS event	MRQ
5.6	The admin portal shall equip with near-real-time Traffic Overview Dashboard including raw, mitigated and clean traffic graphs in bps & pps. The graph should be available hourly, daily, weekly and monthly view.	MRQ
5.7	The admin portal shall be equipped with Traffic Profiling Dashboard for reporting traffic baseline and associated statistics.	MRQ
5.8	The admin portal shall be equipped with Dashboard for site configuration for managed objects configuration and management.	MRQ
5.9	The admin portal should equip with Dashboard for detection and mitigation policy management.	MRQ

5.10	The admin portal shall allow updating of detection / mitigation policies through the web interface and dispatch updates to all corresponding devices within the system.	MRQ
5.11	The admin portal shall log all configuration changes for audit purposes. The audit log shall include: - user submitting the change - date & time stamp of the change - comment of the change The audit log shall be available for retrieval by the authorized users on the admin portal.	MRQ
5.12	The admin portal shall make the customer / admin portal user access log available to authorized users for audit purpose.	MRQ
5.13	The admin portal shall support auto-mitigation templates to associate with individual managed object.	MRQ
5.14	The admin portal should provide an API for integration with 3rd party systems. API shall allow retrieval of information from the Dashboard on the Admin portal including site configuration, DDoS event status as well as detection and mitigation policies.	MRQ
5.15	The admin portal shall support packet capturing and decode of data packets to facilitate mitigation.	MRQ
5.16	All management and integration APIs shall support secure authentication and authorization mechanisms including token-based authentication and TLS version 1.2 or higher.	CRQ
5.17	The system shall retain DDoS detection logs, mitigation logs, audit logs, and configuration logs for a minimum period of twelve (12) months.	CRQ
6.0	Customer portal	
6.1	Customer portal access shall support secure HTTPS access only.	MRQ
6.2	The Customer portal shall support role base access control policy. This policy defines the privilege of access and the authorized action allowed for the customer portal user.	CRQ
6.3	The Customer portal users shall be able to view their managed object/managed entity traffic summary, ongoing and recent alerts, ongoing and recent mitigations. Customers shall be able to view & manage their DDOS alerts, view and manage their managed entities, view and manage their ongoing mitigations through this service portal.	CRQ
6.4	The Customer portal shall be able to support multi tenancy	CRQ
6.5	The Customer portal shall support 2FA.	MRQ
6.6	The Customer portal shall equip with near-real-time Traffic Overview Dashboard including raw, mitigated and clean traffic graphs in bps & pps.	MRQ
6.7	The Customer portal shall equip with DDoS Alert Dashboard for reporting attack events and associated statistics including but not limited to - start time of the attack - size of the attack in bps & pps - duration of the attack - status of the attack - under attack IP address and service ports	MRQ

	- attack type - top 100 traffic patterns - packet size distribution - threat map - IP of router detecting attack - traffic graph during the DDoS event	
6.8	The Customer portal should be equipped with Traffic Profiling Dashboard for reporting traffic baseline and associated statistics.	MRQ
6.9	The Customer portal shall be equipped with Dashboard for site configuration for managed objects configuration and management.	MRQ
6.10	The Customer portal shall equip with Dashboard for detection and mitigation policy management.	MRQ
6.11	The Customer portal provides an API for integration with 3rd party systems. API shall allow retrieval of information from the Dashboard on the Customer portal including site configuration, DDoS event status as well as detection and mitigation policies.	MRQ
6.12	The Customer portal shall generate monthly reports for the subscribed service of each customer.	CRQ
6.13	The Customer portal shall have the past 12 monthly reports available for web access and retrieval at any time.	MRQ
6.14	The system shall generate detailed post-incident reports for major DDoS attacks, including attack vectors, duration, mitigation actions taken, and recommendations.	CRQ
6.15	The system should provide executive-level summary reports suitable for management and regulatory reporting.	MRQ
7.0	Project Management and Services scope	
	The bidder shall be responsible for the project management of the service. The duties of project management services shall include the following:	
7.1	The bidder shall include Project Management including Design, Planning, Deployment, Testing and UAT of DDoS Appliance. Delivered by bidder and technology vendor Project Manager.	CRQ
7.2	The bidder shall be responsible for configuring the network routers as part of the integration process with the DDoS Detection and Mitigation system to ensure seamless traffic redirection, detection accuracy, and effective mitigation.	CRQ
7.3	The bidder must provide an expert certified engineer (JNCIE/CCIE/HCIE *Service Provider*) during integration.	REQ
7.4	Bidder to be responsible for the total project management and act as a single contact point regarding all related activities;	REQ
7.5	Take the lead in coordinating various parties for the smooth implementation of the service;	REQ
7.6	Resolve conflicts during the entire project life cycle;	REQ
7.7	Oversee and monitor the progress of various activities during the project life cycle to ensure that these activities have been completed according to the implementation schedule and comply with all mandatory requirements;	REQ

<table>
<tr><td>7.8</td><td>Plan and schedule meetings at appropriate time during the project life cycle</td><td>REQ</td></tr>
<tr><td>7.9</td><td>Report progress, follow up all outstanding issues with all related parties, suggest solutions and resolve difficulties throughout the project life cycle; and</td><td>REQ</td></tr>
<tr><td>7.10</td><td>Any other activities which are necessary for the satisfactory completion of the service.</td><td>REQ</td></tr>
<tr><td>7.11</td><td>The bidder must provide full Managed Security Services that includes 24x7 SOC with a maximum response time of fifteen (15) minutes from confirmed DDoS detection.</td><td>CRQ</td></tr>
<tr><td>7.12</td><td>The vendor shall provide necessary training to empower Allo's operation team to be able to handle own monitoring</td><td>CRQ</td></tr>
<tr><td>7.13</td><td>The system shall initiate mitigation automatically within sixty (60) seconds upon confirmed DDoS attack detection.</td><td>CRQ</td></tr>
<tr><td>7.14</td><td>The bidder shall provide continuous software updates, attack signature updates, and threat intelligence feeds for the duration of the contract at no additional cost.</td><td>CRQ</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>8</td><td>Service Level Agreement (SLA)</td><td></td></tr>
<tr><td></td><td>The bidder must comply with the specified SLA requirements (applies to Managed Security Services and technical support) to ensure timely incident handling, service restoration, and proper reporting, as outlined in the table below:</td><td></td></tr>
<tr><td>8.1</td><td>
<table>
<tr><th></th><th></th><th colspan="2">Solution</th><th colspan="2">Report Submission</th></tr>
<tr><th>Fault Severity</th><th>Response Time</th><th>Restore Time</th><th>Resolve Time</th><th>Initial</th><th>Final</th></tr>
<tr><td>Critical</td><td>Immediately (within 15 minutes)</td><td>2 Hours</td><td>5 Business Days</td><td>24 Hours</td><td>7 Business Days</td></tr>
<tr><td>Major</td><td>15 minutes</td><td>4 Hours</td><td>7 Business Days</td><td>Next Business Day</td><td>14 Business Days</td></tr>
<tr><td>Minor</td><td>24 hours</td><td>7 Business Days</td><td>14 Business Days</td><td>10 Business Days</td><td>30 Business Days</td></tr>
</table>
</td><td>MRQ</td></tr>
</table>

I acknowledge that I have read, understand and comply with the above Provision of Statement of Compliance ("SOC") and Scope of Works ("SoW") and capable of performing all of the stated requirements.
Name:
Designation:
Company Name:
Company Stamp:
Date:

APPENDIX A

Table 1: DDoS Incident Severity Definitions

Severity	Description
HIGH	Active large-scale DDoS attack resulting in **complete service outage**, severe network congestion, or total unavailability of protected services. Immediate mitigation and escalation are required to restore availability.
MEDIUM	Moderate DDoS activity or abnormal traffic patterns that are **partially mitigated** and have limited customer impact. May escalate if traffic volume increases or persists.
LOW	Low-rate DDoS attempts, reconnaissance traffic, or attack indicators **successfully mitigated automatically** with no noticeable impact on service availability.

---

2. Service Level Agreement (SLA)

2.1 Incident Management (DDoS)

Method of Communication

- Phone Call
- Email Support
- WhatsApp (for operational escalation)

Table 2: Incident Response & Escalation SLA (DDoS)

Severity	Incident Handling	Escalation to PIC	Response & Notification Commitment	Compliance / Notes
HIGH	Immediate	Yes	Notify PIC **within 30 minutes** upon validation via phone call. DDoS mitigation activated. Findings and remediation plan provided via incident email ticket.	SLA monitored monthly.

MEDIUM	Immediate	Yes	Notify PIC **within 60 minutes** via incident email ticket with initial findings and mitigation actions. Escalation if attack severity increases.	SLA monitored monthly.
LOW	Within 24 hours	No (unless repeated)	No immediate contact required. Incident logged. If multiple or rapid occurrences detected, PIC notified **within 3 hours** via email with findings and actions taken.	SLA monitored monthly.

---

3. Restoration & Availability SLA (DDoS)

Table 3: DDoS Service Availability & Service Credits

Severity	Target Restoration Time (MTTR)	Service Level Availability (Monthly)	Service Credit / Rebate
HIGH	≤ **4 Hours**	**99.5%**	Percentage deduction from Monthly Service Fee (MSF) per breach, capped at **10% of MSF per month**
MEDIUM	≤ **8 Hours**	**99.0%**	Percentage deduction from MSF per breach, capped at **5% of MSF per month**
LOW	Best effort	**≥ 95.0%**	Percentage deduction from MSF per breach, capped at **3% of MSF per month**

APPENDIX TO PURCHASE ORDER TERMS AND CONDITIONS

<table>
<tr><th>ITEM</th><th>CLAUSE</th><th>DESCRIPTION</th></tr>
<tr><td>Payment Terms</td><td>4</td><td>
<table>
<tr><th>No.</th><th>Progress Payment</th><th>Accumulative Progress Payment</th><th>Conditions</th></tr>
<tr><td>1.</td><td>100%</td><td>100%</td><td>End month of every quarter with verification by Project Manager</td></tr>
</table>
</td></tr>
<tr><td>Performance Bond</td><td>6</td><td>Not Applicable</td></tr>
<tr><td>Warranty Period (If applicable)</td><td>9</td><td><u>Option 1: 1-year purchase</u>
Twelve (12) months

<u>Option 2: 2-years purchase</u>
Twenty-four (24) months

<u>Option 3: 3-years purchase</u>
Thirty-six (36) months</td></tr>
<tr><td>Insurance</td><td>11</td><td>1. Public Liability Insurance with a minimum coverage of RM500,000 per occurrence, to cover any loss, damage, or injury to third parties or property arising out of or in connection with the performance of the Works.

2. Workmen’s Compensation Insurance of fifteen percent (15%) of the Contract Price covering all personnel engaged by the Contractor for the performance of the Works.</td></tr>
<tr><td>Defects Liability Period (If applicable)</td><td>12</td><td>Not Applicable</td></tr>
<tr><td>Liquidated Damages</td><td>15</td><td>To refer Appendix A of Service Level Agreement (SLA)</td></tr>
<tr><td>Special Terms and Conditions</td><td>30</td><td>Not Applicable</td></tr>
</table>