ANNEX B

SCOPE OF REQUIREMENT

OBJECTIVE OF SOR

1. SAFYC requires the service of a company to supply the below ICT Security Monitoring for SAFYC-Sembawang, 43, Admiralty Road West.

2. The quotation should include the below list of items/works/services to be completed and/or delivered.

3. The broad timeline is as follows:

   a. Tender start on 02 May 2025

   b. Tender closed on 21 May 2025 6 pm.

   c. Tender evaluation and award of tender by last week of May 2025

   d. Delivery from 31 Jul 2025 onwards

SCOPE OF REQUIREMENTS

4. Scope of Work

General Requirements
a. The Contractor shall provide 24x7 security detection and monitoring service for Customers. This shall include consolidating, correlating and prioritising logs/alerts from Customers to accurately identify impending or on-going attacks on Customers' networks and systems.

b. The Contractor shall provide a secure channel to transmit logs/alerts between the Customer's environment and the Contractor's Security Operating Centre (SOC). The transmission shall be secured with IPSEC VPN. There shall also be safeguards in place to ensure the logs/alerts are not lost in event that the link is down.

c. The log/alert sources shall include (but not limited to) operating systems, server software, client applications, network/security software and appliances. The Contractor shall provide an option to process proprietary logs/alerts.

d. The Contractor shall ensure the detection of cyber attacks is augmented by correlating with intelligence feeds from various sources including those of the Authority. The Contractor shall work with the Authority on the procedures for obtaining such feeds.

e. The Contractor shall track traffic profile over time to improve the likelihood of detecting anomalous traffic patterns including (but not limited to) huge data outflow (i.e. data exfiltration), privileged account access from Internet and lateral movement.

f. The Contractor shall perform analysis of the attack trends and maintain information on suspicious attack sources for long term correlation.

g. The Contractor shall provide information on the attacking host(s) where applicable. At a minimum, the following activities shall be performed to facilitate attack host identification.

i. Validating the Attacking Host’s IP Address

ii. Researching the Attacking Host through Search Engines

iii. Using Incident Databases

iv. Monitoring Possible Attacker Communication Channels

h. The Contractor shall work with Authority and Customers to fine-tune the correlation rules and signatures to accurately identify impending or on-going attacks.

i. The Contractor shall ensure rules and signature updates to detect/block vulnerabilities are implemented in a timely manner based on the following schedule:

Criticality Level	**Service Levels**
High	- Interim signature to be in place within one (1) day after vulnerability has been announced. - Official signature to be installed within twelve (12) hours after it has been released.
Medium	- Interim signature to be in place at within one (1) week after vulnerability has been announced. - Official signature to be installed within one (1) week after it has been released.
Low	- Interim signature to be in place within two (2) weeks after vulnerability has been announced. - Official signature to be installed within one (1) week after it has been released.

j. The Contractor shall work with the Authority to adopt an Incident Response Framework. The Contractor shall notify, escalate and resolve security incidents based on this framework.

The Contractor shall also make the necessary assessment and recommendation for the Customer to close the incident.

k. The Contractor shall work with the Authority and Customers to develop and adopt an Incident Response Playbook. The playbook will enumerate the various cyber incidents and their containment strategies (e.g. blacklist offending IP addresses, quarantine server).

l. The Contractor shall provide Security Information and Event Management (SIEM) access for Authority. The SIEM shall allow customised dashboard and provide full log access allowing Authority to conduct their own queries.

m. The Contractor shall provide Authority with the Indicators of Compromise discovered as a result of monitoring Customers' networks and systems.

n. The Contractor shall provide monthly reports tailored to each Customer summarising the state of cybersecurity for their respective networks and systems. The Contractor shall minimally include the following information within the report:

i. Customer Threat Landscape
ii. Security Incident Summary (includes malware incidents)
iii. Traffic Analysis (e.g. intrusion attempts, traffic profile, etc)
iv. Security Patch Status
v. Case Studies (for significant incidents)
vi. Other Significant Observations or Anomalies
vii. Rules, signatures and configuration changes

o. The Contractor shall allow free transfer to monitor another similar device under the Service. The Customer can use this transfer in situations where the monitored system will be re-deployed or decommissioned.
p. The Contractor shall provide Customers' logs/alerts and incident data to Authority upon request at no additional cost. The Contractor shall ensure that the logs can be readable in ASCII plaintext or UTF-8 and work with the Authority on the procedures for such requests. The request shall be granted based on the following schedule.

Age of Data	**Service Level**
Data up to three (3) months old	Within one (1) day of request
Data older than three (3) months old	Within five (5) days of request

q. The Contractor shall not have more than an overall total of five (5) false negative security incidents per calendar year.
r. The Contractor shall not have more than 10% false negative incidents per Customer per month.
s. The Contractor shall not have more than 10% false positive incident escalations per Customer per month.
t. Implementation timeline. To continue the 24/7 ICT security monitoring after 30 Jul 2025.

5. SUBMISSION OF DOCUMENTS

Interested suppliers shall submit the following documents for evaluation purpose:

i. Quotation, including all costs associated with the deliverables must be included and specified.
ii. Company track record, relevant experience, quality and timeliness of service, ability to deliver and financial stability.

a. Tender returns are to be submitted to SAFYC in sealed envelope. Address : 43 Admiralty Road West Singapore 759962

10. Any clarification to the above scope of requirements, please contact SAFYC's representative – Peggy Fam at 63519161 or email peggy@safyc.org.sg with Subject Matter: **ICT Security Monitoring Tender**

11. CRITICAL CRITERIA

a. Supplier shall ensure the completeness of price proposal for Firm/Option Requirement. It is mandatory for Suppliers to complete and submit the price proposal in accordance to the Price Format in Annex A.

12. OTHER CRITERIA

a. Suppliers' quotation shall be evaluated based on compliance to requirement specifications as specified in Annex B.

13. Notes:

a. The prices quoted above shall be exclusive of GST.

b. This quotation complies with all of SAFYC's requirements unless qualified otherwise.

c. All costs associated with the deliverables must be included and specified.

d. No extra cost is to be incurred in addition to the quoted price, inclusive of transport and other charges.

e. SAFYC shall make payment within 30 days upon completion of service and receipt of the invoice upon completion of services. No advance deposit shall be paid.