

## **TERMS OF REFERENCE**

### **SUPPLY, INSTALLATION, TESTING, AND COMMISSIONING OF QUEZON CITY CYBERSECURITY SYSTEM - PHASE 2**

#### **I. PROJECT BACKGROUND, DESCRIPTION AND OBJECTIVES**

##### **a. Rationale**

Quezon City Local Government has been recognized for its best practices in digital transformation, providing efficient and modern public services to its constituents and the citizens of the Philippines.

Like any other city, Quezon City handles sensitive information, such as citizens' personal details, financial data, and other confidential records, which must be safeguarded against unauthorized access.

Given the complex information systems and the interconnection of various offices and departments within Quezon City LGU, the city seeks to engage a qualified third-party service provider. This provider will design and implement a cybersecurity solution that is efficient, comprehensive, and secure.

As cyberattacks grow more frequent and sophisticated, they present significant risks to the city's infrastructure, disrupt essential services, and result in financial losses. Therefore, it is essential to implement effective cybersecurity measures to prevent these attacks and mitigate their potential impact.

Cybersecurity is critical for Quezon City to safeguard sensitive data, avert cyberattacks, comply with regulatory requirements, and uphold its reputation.

##### **b. Objectives**

- i. To enhance the city's security posture by improving measures that protect sensitive information and systems.
- ii. To reduce risks by minimizing the likelihood of data breaches, cyberattacks, and other security incidents.
- iii. To improve compliance by ensuring adherence to industry standards and regulations.
- iv. To establish a faster incident response by implementing efficient processes to promptly address security threats.

#### **II. Scope of Work and Deliverables**

The service provider shall deliver the following:

##### **a. Security Command Center - Enterprise License**

- i. Multi-Cloud Coverage (GCP, AWS, Azure)
- ii. Cloud Security Posture Management
- iii. Cloud Workload Protection Program
- iv. Cloud Security Compliance
- v. Cloud Attack Path Simulation
- vi. Cloud Virtual Red Teaming
- vii. Cloud Infrastructure as Code (IaC) validation
- viii. Cloud Infrastructure Entitlement Monitoring
- ix. Enterprise Security Operations,
  - 1. Threat detection
  - 2. Investigation
  - 3. Response capabilities with case management and automated playbooks
- x. Integrated Cloud threat intelligence
- xi. Integrated AI summarization of reports
- xii. IT service management platform integration

**b. MSSP + SecOps Capability-Building**

- i. The service provider will conduct bi-monthly web scans on 60+ web applications to identify vulnerabilities and protect web assets.
  - 1. Web scanning must be performed bi-monthly utilizing the Cloud Web Security Scanner.
- ii. The service provider will collaborate with QC-ITDD and deliver the following plans:
  - 1. Cloud Infra Organization Policy current state review and implementation.
  - 2. Cloud Resource Hierarchy review and changes/implementation.
  - 3. Cloud IAM policy review and changes/implementation.
  - 4. Cloud Network review and changes/implementation.
  - 5. Data and Storage review and security posture improvement
  - 6. Compute engine review and security posture improvement.
  - 7. Backup and DR review/recommendations
  - 8. Load balancer review and Cloud Armor rules recommendations/implementation.
  - 9. Kubernetes setup review and security recommendations/implementation for posture improvement.
- iii. The service provider will implement the following:
  - 1. Security Management and Optimization: 24/7/365 monitoring and management of security threats. Implement and improve security policies to comply with relevant standards. Keep systems up-to-date with security patches to minimize vulnerabilities.

2. Security Posture Assessments: Identify vulnerabilities, remediate, continuously refine security strategy and adapt to evolving threats.
- iv. The service provider will deliver comprehensive training programs to equip QC-ITDD's cybersecurity personnel with the knowledge and skills necessary to effectively utilize the Security Command Center. These training sessions cover a wide range of topics, including platform navigation, configuration options, alert management, and best practices.
- v. The Service Provider will provide the following capacity-building initiatives:
  1. To assist in the creation of a dedicated Security Operations (SecOps) team within the Quezon City Local Government (QC-LGU).
  2. To provide comprehensive training and knowledge transfer to the newly formed SecOps team, ensuring their proficiency in cybersecurity practices.
  3. Evaluate existing security procedures and knowledge base to identify areas for improvement.
  4. Create new security procedures and knowledge base entries to address identified gaps and enhance the team's capabilities.

**c. Incident Response Retainer (40 Units)**

The Principal Service Provider shall deliver the following:

- i. Computer security incident response support
- ii. Digital forensics, log, and malware analysis support
- iii. Incident remediation assistance
- iv. Respond to requests within a maximum of four (4) hours
- v. On scope agreement, an Incident Response Lead will be assigned within twenty-four (24) hours
- vi. Ability to provide technologies to perform further in depth investigation.
- vii. All work activities will be performed without day and time restrictions.
- viii. The following Deliverables may be produced for Incident Response Services:
  1. Incident Response Service Status Reporting – During the engagement, the Principal Service Provider will provide weekly status reporting that will summarize activities completed, key engagement statistics, issues requiring attention and plans for the next reporting period.
  2. Incident Response Service Final Report – Upon completion of any Incident Response Service engagement, The Principal Service Provider will provide a detailed final report covering

the engagement activities, results and recommendations for remediation in a written detailed technical document.

3. Incident Response Service Executive Briefing – Upon completion of any Incident Response Service engagement and as required to inform senior executives or board level members, the Principal Service Provider will provide an executive brief that summarizes engagement results and recommendations in executive format.
- ix. Any unused IRR units at the end of the year may be reallocated to other expertise on demand services, such as red teaming and tabletop exercises.

### **III. PROJECT STANDARDS AND REQUIREMENTS**

The following are the minimum qualifications and requirements for the Supplier or Bidder:

#### **a. Track Record**

- i. The service provider must be in the same industry as per their Department of Trade and Industry (DTI) Securities and Exchange Commission (SEC) or filing for at least ten (10) years.
- ii. The service provider must be an operational company for at least ten (10) years.
- iii. The service provider must have satisfactorily implemented a similar project “testing and commissioning a cybersecurity system for Quezon City LGU” within the last one (1) year.
- iv. The service provider should have implemented a public sector cloud-hosting web application firewall and security services project with a single completed contract amounting to at least fifty percent (50%) of the ABC.

#### **b. Organization**

- i. The service provider must have updated Platinum status in PHILGEPS.
- ii. The service provider must be a duly registered corporation with an SEC filing.
- iii. The service provider must be filed with SEC or DTI as an IT company with the purpose of software development and the supply of IT-related goods and services.
- iv. The service provider must have an active and updated registration with the National Privacy Commission.

- v. The service provider must be a PREMIER/highest level partnership certificate. The bidder will be required to submit an appropriate Partnership Level certification from its associated Principal Service Provider.
- vi. The service provider must be a Partner Advantage SecOps Reseller. The bidder will be required to submit an appropriate document or proof from its associated Principal Service Provider.

**c. Principal Service Provider Capabilities**

- i. The Principal Service Provider must have at least 15 years of experience in incident response and forensic investigations related to cyber security across various countries and verticals.
- ii. The Principal Service Provider must have a global team of consultants of 300 or more dedicated to incident response and compromised assessment.
- iii. The Principal Service Provider must have a global team of incident investigators located in at least 20 countries.
- iv. The Principal Service Provider must have its own Threat Intel Team of at least 200 or more cyber threat intelligence analysts generating market leading intel.
- v. The Principal Service Provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorized by specific APT groups.
- vi. The Principal Service Provider must be rated a Leader in Incident Response by Forrester Wave (Q1 2022).
- vii. The Principal Service Provider must be rated a Leader in External Threat Intelligence Services by Forrester Wave (Q3 2023).

**d. Manpower Requirements**

The proposed project team must consist of qualified experts and specialists, as outlined in the following table. A minimum of four (4) distinct individuals are required, ensuring that there is no duplication of roles. However, the service provider may augment the team with additional personnel if deemed necessary to effectively execute the project.

The bid document must include comprehensive curriculum vitae or any equivalent for all proposed team members, highlighting their relevant experience in information systems and cybersecurity practices.

- a. One (1) Project Manager
  - i. At least four (4) years experience in managing IT related projects; solutioning of cyber security threats.
  - ii. Graduate of any 4-year computer course or IT related course.
  - iii. Must have a certificate on Cloud Digital Leader or a connected Project Management discipline.

- b. One (1) Security Engineer**
  - i. At least three (3) years experience in solving cyber security threats.
  - ii. Graduate of any 4-year computer course or IT related course.
  - iii. Must have a certificate on Professional Cloud Security Engineer or a connected Cybersecurity discipline.
- c. At Least Two (2) Incident Response Specialists/ Experts from the Principal Service Provider**
  - i. Experience with cybersecurity tools: Familiarity with network traffic analyzers, endpoint protection solutions, intrusion detection systems, and security information and event management (SIEM) systems.
  - ii. Mastery of various operating systems: Demonstrated expertise in Windows, Linux, and macOS.
  - iii. In-depth comprehension of cybersecurity principles: Including proficiency in network security, endpoint security, cloud security, threat intelligence, and digital forensics.
  - iv. Substantial hands-on experience in incident response: Demonstrated ability to handle a variety of cyberattacks, including data breaches, ransomware, and malware infections.
  - v. Experience with threat intelligence: A solid understanding of threat actors, tactics, techniques, and procedures (TTPs).

**d. Additional Documents**

- i. DPO Officer certified by NPC
- ii. Valid National Privacy Commission Certificate or Official Receipt as proof of renewal for CY 2024.
- iii. The bidder must have the following certifications/ credentials:
  - 1. Three (3) SecOps Technical Credentials
  - 2. Three (3) Professional Cloud Architect
  - 3. Seven (7) Professional Cloud Developer
  - 4. Ten (10) Certified Cloud Digital Leader

**IV. PROJECT DEVELOPMENT AND DEPLOYMENT DURATION**

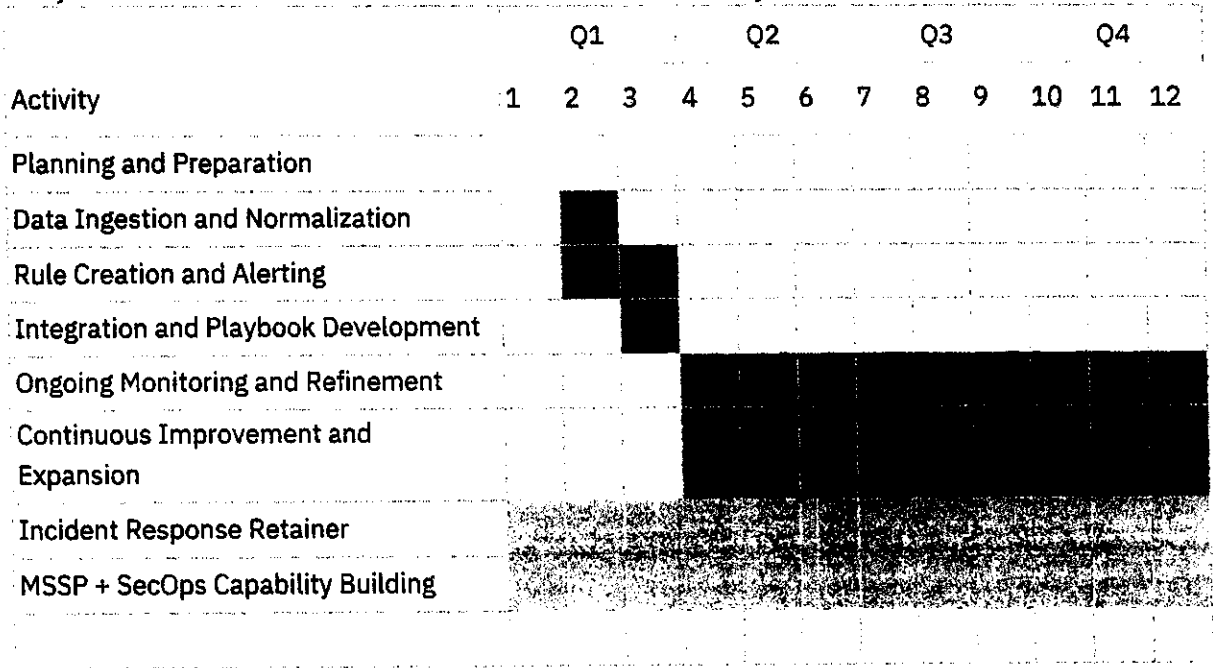
The contract duration shall be twelve (12) months commencing on the date of execution. Throughout the contract period, the service provider shall maintain a collaborative partnership with the Quezon City Information Technology Development Department's cybersecurity team.

While on-site visits are not a contractual requirement, the service provider is committed to regular engagement with the Quezon City Local Government Unit and relevant departments. This engagement will encompass meetings, workshops, and

other appropriate communication channels to ensure timely updates, support, and alignment with the City's cybersecurity strategic objectives.

**Project Implementation Plan**

Project Timeline: Twelve months or 365 calendar days



**V. APPROVED BUDGET COST**

The Approved Budget for this Contract (ABC) amounts to Twenty One Million Pesos (P21,000,000.00) , inclusive of Value-Added Tax (VAT).

**VI. DELIVERY AND PAYMENT SCHEDULE**

The project shall be paid on the schedule indicated below:

Description	Deliverables	Schedule of Delivery
<b>MILESTONE 1</b> <ul style="list-style-type: none"><li>Payment equivalent to 50% of the contract amount shall be made upon Conduct of Project Kick-off and submission of Project Inception Report</li></ul>	<ul style="list-style-type: none"><li>Conduct of Project Kick-off, and</li><li>Submission of Project Inception Report</li></ul>	Within Fifteen (15) calendar days upon receipt of notice to Proceed (NTP)
<b>MILESTONE 2</b> <ul style="list-style-type: none"><li>Payment equivalent to 20% of the contract amount shall be made upon Submission of Proof of the Deployment and Completion of Provisioning, Installation, Configuration and Testing of Security Command Center (QC SCC) Enterprise Software License, Incident</li></ul>	<ul style="list-style-type: none"><li>Proof of Delivery of Quezon City Security Command Center (QC SCC) Enterprise Software License</li><li>Completion of Provisioning, Installation, Configuration and Testing of Security Command</li></ul>	Within Ninety (90) calendar days upon receipt of notice to Proceed (NTP)

Response Retainer Access, and MSSP accomplishments.	Center (QC SCC) Enterprise Software License <ul style="list-style-type: none"> <li>▪ Proof of Incident Response Retainer Access (Service Agreement/ Contract)</li> <li>▪ Security Posture and Vulnerability Assessment Reports</li> </ul>	
<b>MILESTONE 3</b> <ul style="list-style-type: none"> <li>▪ Payment equivalent to 20% of the contract amount shall be made upon the Conduct of Training, Knowledge Transfer, and Submission of Project Completion Document.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Trainings/ Workshops (SCC and SecOps Capability-Building)</li> <li>▪ Conduct of Knowledge Transfer</li> </ul>	Within One Hundred Eighty (180) calendar days upon receipt of notice to Proceed (NTP)
<b>MILESTONE 4</b> <ul style="list-style-type: none"> <li>▪ Payment equivalent to 10% of the contract amount shall be made upon Submission of Project Completion Documents.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Submission of Project Completion Documents</li> </ul>	Within Three Sixty (360) calendar days upon receipt of notice to Proceed (NTP)

Delivery must be in **Quezon City Government, Quezon City Hall Compound, Elliptical Road, Diliman, Quezon City, Metro Manila.**

**VII. BASIS OF PAYMENT**

Upon the QC-ITDD's official verification or confirmation of the successful deployment, implementation, or delivery of a completed milestone, the QC - ITDD will authorize the full payment of the corresponding milestone perce, as stipulated in the DELIVERY AND PAYMENT SCHEDULE.


**VIII. PENALTIES FOR BREACH OF CONTRACT**

Failure to deliver the services according to the standards and requirements set by the City shall constitute an offense and shall subject the Contractor to penalties and/or liquidated damages pursuant to RA 9184 and its revised Implementing Rules and Regulations.

**IX. CANCELLATION OR TERMINATION OF CONTRACT**

The guidelines contained in RA 9184 and its revised IRR shall be followed in the termination of any service contract. In the event the City terminated the Contract due to default insolvency, or for cause, it may enter negotiated procurement pursuant to section 53 (d) of RA 9184 and its IRR.

Approved by:

  
**PAUL RENE S. PADILLA**  
 Head, QC-ITDD





REPUBLIC OF THE PHILIPPINES  
QUEZON CITY  
INFORMATION TECHNOLOGY  
DEVELOPMENT DEPARTMENT



COST DERIVATION  
CYBERSECURITY SYSTEM

Item No.	ITEM DESCRIPTION/SPECIFICATION	UNIT	QTY.	UNIT COST	TOTAL COST
1	<b>SECURITY COMMAND CENTER - Enterprise</b> Multi-Cloud Coverage (GCP, AWS, Azure) Cloud Security Posture Management Cloud Workload Protection Program Cloud Security Compliance Cloud Attack Path Simulation Cloud Virtual Red Teaming Cloud Infrastructure as Code (IaC) validation Cloud Infrastructure Entitlement Monitoring Enterprise Security Operations, Threat detection & Investigation Response capabilities with case management and automated playbooks Integrated Cloud threat intelligence Integrated AI summarization of reports IT service management platform integration	License	1	4,200,000.00	4,200,000.00
2	<b>MSSP + SecOps Capability-Building</b> Cloud Web Security Scanning Cloud Infra Organization Policy current state review and implementation. Cloud Resource Hierarchy review and changes/implementation. Cloud IAM policy review and changes/implementation. Cloud Network review and changes/implementation. Data and Storage review and security posture improvement Compute engine review and security posture improvement. Backup and DR review/recommendations Load balancer review and Cloud Armor rules recommendations/implementation. Kubernetes setup review and security recommendations/implementation for posture improvement. Security Management and Optimization with 24/7/365 monitoring and management of security threats. Security Posture Assessments Comprehensive training programs to effectively utilize the Security Command Center. QC LGU Internal Security Operations (SecOps) Capability-Building	Lot	1	₱11,800,000.00	11,800,000.00
3	<b>Incident Response Retainer</b> Computer security incident response support Digital forensics, log, and malware analysis support Incident remediation assistance Provide technologies to perform further in depth investigation. All work activities will be performed without day and time restrictions. Incident Response Service Status Reporting Incident Response Service Final Report technical document. Incident Response Service Executive Briefing Reallocation of unused units to other expertise on demand services, such as red teaming or cyber security training.	Units	40	₱125,000.00	5,000,000.00
				<b>TOTAL:</b>	<b>PHP 21,000,000.00</b>

Note: Mark-up inclusion: Provision for Inflation, VAT, City Tax, Allowable COA percentage profit for suppliers, Foreign Exchange Rate & Bid document fees;

Terms of Payment : Milestone Payment (1-Year Contract)

Delivery Period : Milestone Delivery (1-Year Contract)

Prepared by:

VICTOR ALLEN M. ROQUE  
CMT II - NTMD

Noted by:

PAUL RENE S. PADILLA  
Head, ITDD