TERMS OF REFERENCE

QUEZON CITY ANTI DRUG ABUSE COUNCIL (QCADAC) SUBSCRIPTION OF INTEGRATED DRUG ABUSE PROFILING SYSTEM DATABASE AND WEBSITE APPLICATION CLOUD HOSTING

I.   BACKGROUND

The Quezon City Anti-Drug Abuse Council (QCADAC) requires ongoing support to ensure that its database, web application, and cloud server infrastructure remain operational, secure, and efficient. This TOR specifies the requirements and responsibilities of the service provider for database, web application, and cloud server maintenance in order to support the QCADAC's efforts in data management, system optimization, and security.

II.   OBJECTIVES

- Ensuring the availability, reliability, and security of the database and web applications.
- Providing continuous cloud server monitoring, maintenance, and optimization.
- Implementing necessary updates, enhancements, and incident response.
- Minimizing downtime and improving system performance.

III.   SCOPE OF WORK

The service provider shall perform the following tasks to ensure the proper maintenance and operation of the database, web application, and cloud server infrastructure:

3.1.   DATABASE MAINTENANCE AND SUPPORT

- Latest MariaDB Version is the current database engine and version, and to be supported
- AWS RDS is the cloud platform where the database is hosted
- There are 2 database servers and databases in-scope
- The Database shall have a 30 days' worth of daily backup
- 1-3 times a year DB restoration test shall be conducted
- Expected SLAs for database-related incidents are categorized based on severity levels. Fastest should be within the hour. The lowest severity level should be within 24 hours.
- Conduct regular database backups, integrity checks, and restoration testing.
- Perform database optimization tasks to improve query performance and resource usage.
- Manage user roles, access levels, and security policies to protect data confidentiality.
- Monitor and resolve database-related incidents and errors.

3.2.   WEB APPLICATION MAINTENANCE

- The tech stack of the application to be supported, and the frameworks used are LAMP, Laravel, React, Node.js

- Two (2) application servers with load balancer; Six (6) application servers on standby/autoscaling; Two (2) database servers with redundancy and backup; 1TB of cloud storage; Cloud caching feature
- Network, Application, Database, and Workstation devices; Automated Scanning and Manual Testing, Penetration Testing are the expected scope and type of vulnerability assessments
- Vulnerability assessment should be conducted annually
- Implement updates and security patches.
- Fix bugs and resolve any issues affecting the web application's functionality.
- Monitor the application's performance to detect and address potential bottlenecks.
- Conduct regular vulnerability assessments and mitigate identified risks.

3.3. CLOUD SERVER MAINTENANCE AND MANAGEMENT

- Accumulated 10 server instances are in-scope
- Network, Application, Database, and Workstation devices; Automated Scanning and Manual Testing, Penetration Testing – SLAs for incident response
- Ensure server uptime and availability through proactive monitoring and maintenance.
- Perform system updates, security patches, and software installations.
- Monitor server resource usage (CPU, memory, storage) and adjust configurations as needed.
- Manage firewall settings, security configurations, and network policies.
- Provide incident response and disaster recovery services in case of system failure or data loss.

3.4. DATA SECURITY AND COMPLIANCE

- Network Infrastructure Security & Data Privacy are the type of security best practices expected for data protection and security.
- Data Privacy Law, Industry standard compliances are the existing regulations and standards for data handling and privacy that are to be expected
- Implement best practices for data protection and system security.
- Comply with relevant regulations and standards for data handling and privacy.
- Conduct periodic security audits.
- Ensure data encryption in transit and at rest.

3.5. TECHNICAL SUPPORT AND SERVICE MANAGEMENT

- The expected SLA for a 'critical issue' which requires 24x7 support is within 1 hour
- Provide 24/7 technical support for critical issues.
- Offer a helpdesk for troubleshooting and user support.
- Maintain a ticketing system to track issues and resolutions.
- Submit monthly service reports summarizing activities, incidents, and resolutions.

IV. PROJECT STANDARDS AND REQUIREMENTS

The selected service provider must meet the following qualifications:

- At least **5 years** of experience in maintaining similar systems, including database, web application, and cloud server infrastructure.
- A proven track record in delivering high-quality maintenance and support services.
- Certified professionals in cloud computing, database administration, and web development.
- Compliance with **Republic Act No. 10173 (Data Privacy Act of 2012)**
- NPC's mandatory registration for data processing systems handling sensitive personal information.

V. PROJECT DURATION WARRANTY

The project shall be until December 31, 2025, upon activation.

VI. APPROVED BUDGET FOR THE CONTRACT

The approved budget for the contract is One Million Nine Hundred Seventy-Six Thousand Two Hundred Forty-Nine Pesos and Ninety-Nine Centavos Only (P 1,976,249.99).

NO PRICE ADJUSTMENT

The Project cost shall be fixed and there shall be no price adjustments applicable for the duration of the contract except when the operations costs are increased bv more than 10% as a result of any extraordinary circumstance as determined by the National Economic Development Authority (NEDA). Pursuant to the provisions of RA 9184 and its IRR on contract price escalation, all contract price escalation shall be approved by the Government Procurement Policy Board (GPPB).

VII. CONFIDENTIALITY

The service provider is required to maintain the confidentiality of all QCADAC data. No information is to be disclosed or shared without written consent from QCADAC. Breach of confidentiality will be subject to contract termination.

VIII. BASIS OF PAYMENT

Full Payment upon activation.

IX. PENALTIES FOR BREACH OF CONTRACT

Failure to deliver the services according to the standards and requirements set by the City shall constitute an offence and shall subject the Contractor to penalties and/or liquidated damages pursuant to RA 9184 and its re vised Implementing Rules and Regulations. Specific penalty/ies to be imposed to the contractor.

X.   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 into negotiated procurement pursuant to section 53 (d) of RA 9184 and its IRR.

Prepared by:

ALFREDO M. FORONDA
Executive Director

Noted by:

HON. GIAN G. SOTTO
City Vice Mayor