

TERMS OF REFERENCE (TOR)**SUPPLY, DELIVERY, INSTALLATION, TESTING AND COMMISSIONING
OF THE OFFICIAL VIOLATION RECEIPT (OVR) MOBILE APPLICATION
AND MAINTENANCE AND UPGRADE OF THE UNIFIED ORDINANCE
VIOLATION REPORT ONLINE ENCODING SYSTEM**

- I. **RATIONALE AND BRIEF BACKGROUND** – With the recent implementation of the Single Ticketing System, there is a pressing need for a mobile application that enables TTMD officers to efficiently issue traffic tickets using mobile devices. This application will also facilitate seamless connectivity with the LTO's LTMS, allowing real-time validation of driver's licenses. To address the evolving operational demands of TTMD, including enhanced integration with the LTMS, increased reliance on online payments, and alignment with QCeServices, the system requires targeted modifications to optimize its functionality. These updates, along with provisions for ongoing hosting and maintenance, are essential to ensure the system remains robust, efficient, and capable of meeting these growing needs.
- II. **PROJECT DESCRIPTION** – The development of the OVR Mobile Application will allow TTMD Deputized Officers to validate a driver's license and issue electronic OVR Traffic Tickets while on the road. The Maintenance and Upgrade of the OVR Online Encoding System will allow TTMD personnel to use the system more effectively and allow for better integration with the LTMS. The continued maintenance and hosting will also allow TTMD personnel to use the system reliably while violators can continue to avail of the online payment option.
- III. **PROJECT STANDARDS AND REQUIREMENTS**

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

- i. **Track Record**
 - a. The service provider must be in the same industry as per their DTI or SEC filing for at least five (5) years
 - b. The service provider should have been in operation for at least five (5) years
 - c. The service provider should have implemented a public or private project with a single completed contract amounting to at least fifty percent (50%) of the ABC.
- ii. **Organization**
 - a. Service providers must have Platinum status in PHILGEPS
 - b. The service provider must be filed with DTI or SEC as an IT company with the purpose of software development and the supply of IT-related goods and services
 - c. The service provider must be duly registered under the National Privacy Commission

- d. The service provider shall guarantee that the system shall abide with the DATA PRIVACY ACT OF 2012 to ensure that the personal information is protected.
- iii. **Manpower**
- a. The service provider must have their own headcount of software developers.
 - b. The service provider must have their own support staff to conduct support tasks for the project such as system administrators and quality assurance testers.
 - c. Staff complement:
 - i. **Overall Project Manager**
 - **Educational Background:** A strong foundation in Computer Science, Computer Engineering, Information Technology, Business Administration, or a related field.
 - **Years of Experience:** Minimum 5-7 years in project management.
 - **Field of Expertise:** Strong background in software development lifecycle (SDLC) management.
 - ii. **Senior Web Developer**
 - **Educational Background:** A strong foundation in Computer Science, Software Engineering, or a related field.
 - **Years of Experience:** Minimum 5-7 years of hands-on experience in web application development, with proven expertise in modern frameworks and technologies.
 - **Field of Expertise:** Full-stack development, API integrations, responsive design, and modern web architecture principles.
 - iii. **Cloud Server Administrator**
 - **Educational Background:** A strong foundation in Information Technology, Computer Science, or related discipline.
 - **Years of Experience:** Minimum 3-5 years of experience managing cloud infrastructures, including deployment, monitoring, and scaling of server resources.
 - **Field of Expertise:** Expertise in Microsoft Azure. Skilled in server virtualization, backup strategies, and disaster recovery planning.
 - iv. **Web Security Engineer**
 - **Educational Background:** A strong foundation in Cybersecurity, Computer Science, or Information Technology.
 - **Years of Experience:** Minimum 2-3 years of experience in web application security and vulnerability assessments.
 - **Field of Expertise:** Proficient in penetration testing and threat analysis. Familiarity with tools like OWASP ZAP is essential.

v. Quality Assurance and Testing Staff

- **Educational Background:** A strong foundation in Computer Science, Information Technology, or related discipline.
- **Years of Experience:** Minimum 2–3 years of experience in software quality assurance and testing.
- **Field of Expertise:** Skilled in creating test plans and in testing processes. Familiarity with bug-tracking systems.

IV. PROJECT SCOPE OF WORK

Technical Specifications:

- a. The Mobile Application must run on a mobile device with the following minimum specifications:
 - a. OS: Android 8.1 or higher
 - b. Memory: 1GB RAM or higher
 - c. Processor: Quad-core 1.3GHz or faster
 - d. Camera: 5MP rear camera or higher
 - e. Display: 5.5" 1280x720 resolution or higher
 - f. Communication: 3G or higher
 - g. WiFi: 802.11b/g/n
 - h. Printer: Thermal Printer
- b. The web applications will store all data collected in a cloud-based repository.
- c. The cloud-based hosting of the data must operate for one (1) year.
- d. The system must allow for periodic backups of the database and must guarantee a 99% database server uptime.
- e. All data captured by the system shall remain the property of the City, and the data will be turned over to the City when the service agreement expires or is terminated with no additional cost to the City
- f. The system software and source code [if custom-built system/application] will be owned by the city and will be turned over to the end-user department or the Information Technology and Development Department (ITDD) [for internal DNS registration (if needed)] at no additional cost upon request or upon termination and non-renewal of any maintenance agreement.

Security:

- a. The web application will have their own secure web server instance inclusive of renewable SSL certificates;
- b. The web applications will implement industry standard measures to protect user data, prevent web fraud, mitigate bot attacks, secure APIs, and prevent unauthorized application access;

System Features:**Mobile Application**

- a. The mobile application should allow authorized users to login by entering their assigned username and password.
- b. The mobile application should allow the user to manually enter the driver's license number and last name. It should then connect to the LTMS to validate the driver's license information and display the driver's violation history and outstanding tickets.
- c. The mobile application should warn the Enforcer if the violator has unpaid tickets, which means the Enforcer can confiscate the driver's license.
- d. The mobile application should allow the user to encode the complete details needed for an OVR traffic ticket, including the Name and Address of the violator, the type of vehicle used, as well as the actual violation(s) committed.
- e. The mobile application should allow the user to attach photos of the driver's license, plate number as well as the actual violation committed.
- f. The mobile application should allow the user to capture the violator's signature or refusal to sign.
- g. The mobile application should allow the user to preview the details of the ticket before printing.
- h. The mobile application should allow the user to print out an electronic OVR traffic ticket using the built-in printer.
- i. The tickets encoded in the Mobile Application should automatically be assigned a ticket number, starting with the "QC" prefix followed by a 3-letter code assigned to each enforcer.

- j. The mobile application should allow the user to reprint the last issued ticket if in case a problem was encountered with the printing.
- k. The mobile application should allow the user to see a summary of previous tickets encoded into the Mobile Application.
- l. The mobile application should have the ability to synchronize with the main system in case there are changes to the list of violations or fines, as well as other field lookup values.
- m. The tickets encoded in the Mobile Application should be visible in the main System.

Enhancements to Deputized Officers Maintenance Module

- n. System should allow the user to easily update a batch of officers to inactive status once their Deputation has expired based on the Expiration Date.
- o. System should display a Deputized Officer (D.O.) Prefix Column in the Officer list Form to allow the user to easily see the assigned Prefix Code that will be used in the ticket numbers assigned to tickets encoded through the Mobile Application.
- p. System should allow the user to easily filter and see which Officers were issued a mobile device.

Enhancements to Violation Maintenance Module

- q. System should allow the user to specify the sort order of the violations so the user can control how it will be sorted in the Mobile Application.

Enhancements to Booklet Issuance Module

- r. System should allow the user to correct the booklet issuance from one officer to another, which should also correct the tickets that were already issued from the same booklet.
- s. System should allow the user to easily see the history of a booklet to see who it was issued to and if it was returned and reissued to another officer.

Enhancements to Ticket Encoding Module

- t. System should allow the user to easily filter the list to only show tickets encoded through the Mobile Application.

- u. When encoding a ticket, the cursor should automatically move to the Specify box/field if the user selects "Others" as the confiscated item.
- v. System should allow the user to indicate if the Vehicle Classification cannot be identified or is not applicable.
- w. System should allow the user to indicate if the Vehicle Type cannot be identified or is not applicable.
- x. The System should have Pedicab as an available option in for the type of vehicle field in the ticket encoding form.
- y. System should have validation to limit the date of apprehension to a specified number of days from the current date, to help prevent the user from entering an erroneous date.

Enhancements to CTO Portal

- z. The system should hide other online payment records from the CTO Portal once the ticket has already been paid.

Enhancements to Ticket Payment Module

- aa. The System should allow the user to filter the Payment Summary List by several ways:
 - i. Payment Method
 - ii. Tickets with no OR numbers
 - iii. Tickets with Pending Status
 - iv. Tickets with Paid Status
 - v. By OR Date
- bb. The System should allow the user to try and retrieve the OR Numbers from the CTO POS by batch.
- cc. The System should allow the user to try and retrieve the OR Numbers from the CTO POS by batch.

Enhancements to Reporting Module

- dd. System should have a Mobile Ticket Transmittal Report that will list all ticket issued using the Mobile Device.
- ee. System should have a Sync Status Report that will show if a ticket was not yet synced, posted or lifted in the LTMS.

Enhancements to LTMS Integration Module

- ff. The System should allow the user to validate a driver's license with the LTMS by entering any of the following parameter combinations:
 - i. Driver's License Number and Last Name
 - ii. Driver's License Number and Serial Number
- gg. The System should also display the Inbox ID being returned by the LTMS in the Sync Ticket Logs, as this will help investigate any syncing issues between the System and LTMS.
- hh. The System should call the LTMS RELEASE API to lift a ticket with an impounded vehicle, to properly lift the alarm from the violator's record in the LTMS.
- ii. The System should have the ability to Cancel or Dismiss tickets that were already synced to LTO, so that the record will not reflect in the violation history of the driver. The user should enter a reason for Cancelling or Dismissing a ticket.
- jj. The System should have a filter in the Sync Ticket Logs to show Dismissed tickets.
- kk. To prevent data integrity issues, the System should not allow the user to edit the ticket number if it was already synced to the LTMS.
- ll. To prevent data integrity issues with the LTMS, the System should not allow the user to delete a ticket if it was already synced to the LTMS.
- mm. The System should allow the user to easily reset the Access Token that is needed to call the LTMS APIs in case a technical issue is encountered with the Access Token.

V. TRAINING

The service provider will provide the equivalent of three (3) total hours of training necessary for the proper usage of the software system inclusive of system manuals to at least two (2) users of the system as well as one (1) ITDD personnel.

VI. AFTER SALES SUPPORT

One (1) year warranty for software bugs and fixes from date of acceptance.

Technical support:

- i. Workdays from 8AM to 5PM, expect a response within the day or by the next workday.
- ii. Weekends and holidays, expect a response by next workday.

VII. PROJECT DURATION

The project shall be for a period of one (1) year from the issuance of the Certificate of Acceptance.

VIII. DELIVERY SCHEDULE

Sixty (60) calendar days from the issuance of the Notice to Proceed.

IX. APPROVED BUDGET FOR THE CONTRACT

The Approved Budget for this Contract (ABC) amounts to twenty million four hundred thousand Pesos [20, 400, 000 PHP] VAT inclusive.

Due Diligence and System Design	
Software Development Cost	
Mobile Application Module	
Feature and Change Requests to Pre-Existing Modules	
Realignment with upgrades to QCeServices	
System Documentation, Training Module and Training	
Technical and Customer Service Support - 12 months	
Cloud Hosting – 12 months	
TOTAL	

X. BASIS OF PAYMENT

Full payment upon completion of the project.

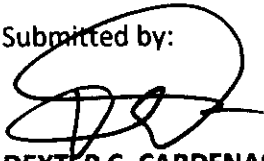
XI. PENALTIES FOR BREACH OF CONTRACT

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 revised Implementing Rules and Regulations.

XII. 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 RA 9184 and its IRR.

Submitted by:



DEXTER C. CARDENAS

Dept. Head, TTMD

Noted:



MARY ANN CRUZ

Chief Information Officer - ITDD



MICHAEL VICTOR N. ALIMURUNG

City Administrator