

TERMS OF REFERENCE (TOR)

ENVIRONMENT INSPECTION SYSTEM SOLUTION FOR THE DEPARTMENT OF SANITATION AND CLEANUP WORKS OF QUEZON CITY (DSQC)

I. PROJECT DESCRIPTION AND OBJECTIVE

The Department of Sanitation and Cleanup Works of Quezon City (DSQC) is the lead department responsible for the City's sanitation and waste management. The DSQC is in-charge of waste collection, processing and issuance of environmental clearances, imposition of environmental ordinance violations, resolving concerns on violations of environmental and sanitary standards, ensuring compliance with environmental laws, related rules and regulations, and general administration of comprehensive environmental protection program.

In 2021, the DSQC subscribed to a mobile software application solution that allows its field personnel doing ocular inspections of business establishments to do the following: print-out violation tickets, view mission orders and route inspection points, fill-out inspection details, and capture photos and videos of the subject of inspection.

Due to the improved performance of the DSQC's personnel resulting from the utilization of this mobile software application, and to further help the DSQC in carrying out its primary mandate, the DSQC deems it necessary to continue using a mobile application solution with advanced features and specifications.

Thus, the DSQC will subscribe to an Environment Inspection System, a software solution in facilitating, managing and monitoring the DSQC's administrative affairs, property management, waste management operations, and permits and compliance. The software solution shall be a service solution and will be connected to a cloud-based Electronic Data Warehouse System (EDW). The EDW will serve not only as a virtual storage space of the DSQC's digital data, but also a data source for completeness check and exception handling and generator of business intelligence reports. The EDW will also facilitate easy search, storage retrieval and cross referencing of information among documents, resulting to simplified work and faster output of the DSQC personnel.

Additionally, the project includes digitizing historical and moving forward documents related to waste management, environmental clearances, compliance records, and other relevant administrative documents. The expected volume for digitization includes backlog years 2022 and 2023 with an estimated volume of 80,000 pages and moving forward documents from 2024.

II. SCOPE OF THE PROJECT/SERVICE PROVIDER DELIVERABLES

Following the receipt of the Notice to Proceed, the Service Provider is expected to provide the following:

a. Deployment and one (1) year subscription to an Environmental Inspection System with the following features and specifications:

1	Environmental Inspection System Module	<ul style="list-style-type: none"> • Ability to print out tickets or documents during field work or inspection conducted by field personnel • Ability to print environmental clearance with QR code that verifies the document against the EDW • Fill out of inspection details • Ability to tag the establishment whether low or high risk, and the classification or nature of the business establishment • Capture the videos or photos of inspection
2	Workflow Module	<ul style="list-style-type: none"> • Workflow tool for generating mission orders • Ability to assign tasks and mission orders to personnel • Ability to monitor the status of tasks and measure the performance of field inspectors • Ability to set resolution to complete/close mission orders • View the list of mission orders • View the route and inspection points plotted on the map • Upload historical mission orders
3	Business Intelligence Reporting Module	<ul style="list-style-type: none"> • Capability to create reports daily, weekly, monthly, quarterly, and annually • Reports generation from data stored in the EDW
4	Verification module	<ul style="list-style-type: none"> • Ability to verify the completeness, consistency and compliance of the submitted documents for environmental clearance per registered business establishment in Quezon City
5	Environmental Ordinance Violation Ticketing Module	<ul style="list-style-type: none"> • Ability to take photos of the violator and his identification card • On-the-spot issuance of Environmental Violation Receipts using existing DSQC's printers with Bluetooth connectivity
6	Interoperability	<ul style="list-style-type: none"> • Ability to integrate with other applications via REST API to get data that relates to inspection results and environmental clearance issuance from the EDW
7	Dashboard	<ul style="list-style-type: none"> • Ability to monitor field inspections and violations • The dashboard must be able to display the following information by district per day, week, month, and quarter: <ul style="list-style-type: none"> ○ Location of inspectors deployed for the day ○ Status of inspections for the day ○ Number of successful inspections ○ Number of EVR ○ Number of individual OTS EVR ○ Number of establishment OTS EVR ○ Number of violations vs inspections

		<ul style="list-style-type: none"> ○ Number of violations per barangay and risk level ○ Statistics on violation being committed by individuals ○ Distribution of establishment per district ○ List of owners and their business establishments ○ Number of low and high-risk establishments vs inspected ● Provide an overview of all data points collected about business establishments
--	--	---

b. Deployment and one (1) year subscription to an Electronic Data Warehouse System with the following system features and functionalities:

Feature Set	Feature	Description
General	Architecture	The system must have a clear separation of the user interface, the application server, the database server and the file storage server to allow for vertical and horizontal scaling. The front end must be web-based to allow users to access the system from any operating system without having to install any applications apart from a browser. The front-end web application must support the most common browsers such as Microsoft Edge, Chrome, Safari and Firefox.
	Multi-type file storage	The system must allow for the storage of various file types including documents, images, videos, audio, URLs and biometric data. The system must allow users to upload all file types except for file types that are potentially dangerous such as executables. The system must not have an inherent limit to the number of files that users can upload into the system. For on-premises deployments, the limit must be imposed only by the available physical storage. For on-cloud deployments, there must be no limit.
	Metadata storage	The system allows for the storage of metadata that corresponds to the files stored in the system to enable search based on the metadata in addition to the name of the file.
	Integration	The system must provide APIs for integration with 3 rd -party software. There must be APIs available to receive files and metadata. There must also be APIs to retrieve files and metadata. The APIs must have a way to ensure that the exchanges between two systems are secure.
Security	Identity and access management	The system must have a facility for creating, updating and deleting user accounts. The system administrator must be able to assign roles to users that determine what features are available to the user. The system must provide for a way to authorize or restrict users to access certain files or folders within the system.

	Login	The web application shall grant access to users via secure log-in using a designated username and password, with the ability to terminate the session through a log-out function, and a password recovery mechanism that is available for forgotten passwords. The web application must provide users a way to login using their biometrics when the device hosting the web application has the appropriate hardware to capture biometric data.
	Restricted files	The system must prevent the upload of potentially dangerous file types such as executable and system files. The list of file types classified as dangerous must be configurable. The manner of determining the file type must be based on the content of the file and not on its file name.
	Anti-virus	The system must prevent the upload of files that are infected by a virus or malware. The system must have a way of updating its virus signatures database so that the system keeps current on the most recent virus or malware.
	Access rights	The system must allow for granular control over what files users or groups of users can access. The level of granularity must be such that a file can be made accessible only to one user. The system must also be flexible enough, such that one or more groups of users can be provided access to a file. The system must also be able to differentiate between read-only access and write/edit access.
	Role access	The system must be able to prevent users from accessing certain features within the system based on the roles assigned to them.
	Vulnerabilities	The system must have undergone a vulnerability assessment and penetration testing by a reputable third-party. The system must not have any critical nor high vulnerabilities as evidenced by the test report submitted by the third-party. The major version of the software indicated in the report must match the major version to be delivered.
	Encryption	The system must enforce encryption of data while data is in transit. The system must also support the encryption of data while data is in storage. The encryption algorithm used must be industry standard.
	Document signing	The system must provide users a means to apply a digital signature to applicable documents such as PDF. The digital signature must be based on an industry standard encryption algorithm which 3 rd -party software can recognize and validate.
	File integrity	The system must store the hash signature of a file when it was uploaded. The hash can be used as evidence of tampering. The hash algorithm must be an industry standard hashing algorithm such as MD5, SHA-1 or SHA-2.

Upload	File, metadata and URL upload	The system must provide a means to upload multiple files at a time. The system must be robust enough to handle temporary and brief loss of connectivity. The system must provide users with an indication of the overall progress of the uploading activity. The system must also provide users a means to upload in bulk the metadata associated with the files. The system must also provide users a means to upload in bulk URLs and their associated metadata.
	Processing	The system must be able to associate processes to files that are being uploaded. The processes applied to files must be rule-based. The system must have built-in processes for file conversions such as TIFF or PDF, and optical character recognition. The processes must be extensible by means of APIs.
	Quality Assurance	The system must provide a means for the user to review encoded indices, shown side by side with corresponding document image and correct exceptions before upload.
Content Management	Data organization	The system must allow users to organize files into folders and subfolders in any way deemed suitable for their use. There must not be any practical limit to the number of folders and subfolders that users can create. The system must also allow the users to reorganize the files at some future time should the need arise. The system must also present the metadata associated with each file. The system must allow users to edit the metadata provided that they have the proper access rights to the file. The user interface must remain responsive regardless of the volume of files contained in a folder.
	User experience	The system must provide users with an efficient way of browsing folders and their content. The system must provide for a means for users to view the following file types without the need to invoke an external program: TIFF, PDF, DOCX, MP4, JPEG, PNG, TXT, XML, and JSON formats. The system must display files and their corresponding metadata such that the association is evident to the user. The system must automatically extract file information such as file size, number of pages, and image resolution where applicable.
	Mobility	The system must have a mobile application that allows users to perform basic functions, such as upload files, search files and view files while on-the-go.
	File management	The system must provide a means for users to create folders, upload files, rename files, move files from one folder to another, delete files and restore deleted files. The system must also provide a means for users to be able to modify the access restrictions of a file or folder directly or by reassigning the file or folder to a different owner or group. The system must also provide a means for users to add, edit or delete associated metadata of any file.

	Version control	The system must provide a means of keeping track of versions of a file. The system must allow users to view any of a file's previous versions.
	Personalization	The system must provide for a means to users to personalize their interaction with the system by way of keeping track of their most recently accessed files, by way of tagging files that are important to them, and by way of customizing the attributes of files that are displayed on screen.
Search	Basic search	The system must support keyword search, exact string search and substring search on the files' file name and content. The system must also allow users to search using multiple keywords, phrases and any combination of both using Boolean operators. The system must also provide a means for users to narrow down the search by using the files' other properties, such as file size and create date. The system must return the search results in order of relevance. The system must be able to automatically highlight the search keyword in the document to show evidence of the presence of the matching text.
	Advanced search	The system must support approximate string-matching search (also called "fuzzy search"). The system must be able to match strings that are sufficiently close to the actual string embedded in the documents or the actual string of the filename. The system must also allow users to use wildcards when using keyword search.
	Content search	The system should automatically extract the text content of documents uploaded into it to allow users to search for documents based on their content. In addition, the system should automatically crawl the URLs uploaded into it to allow users to search the web content.
	Artificial Intelligence	The system must allow users to search based on the meaning of the content. This is also known as "AI Search" or "Semantic Search". The actual search keywords need not be present in the document for the system to identify a match. The meaning of the search keywords only needs to match the meaning of the content of the document. The system must be able to receive search queries and deliver responses in natural language. The responses must also provide links to the documents that support the responses. The system must be able to bring the user to the exact page of the document where the response was based on.
Reports	Metrics	The system must have a report that shows a summary of the content of the system in terms of number of folders, subfolders, files and total number of pages of documents. The system must provide a means to filter out the report by folder or by metadata. The system must have a report that shows statistics on usage of the system.
	Duplicate files	The system must be able to provide a report that determines duplicate files based on their hash signatures.

	Audit	The system must record all activities that users perform on the system. The system must provide reports for user activities. The report must be able to provide information on who accessed a file, what file was accessed, when the file was accessed, what type of action was performed, and from what IP address the action was performed from. The system must provide a means for users to export this information into other systems for further analysis.
--	-------	--

The EDW shall be available for only 100 users. The number of downloads will be limited to 1TB per month. Any excess will be for the account of the DSQC. The EDW shall be able to accommodate up to 100,000 business establishments records and their corresponding supporting documents, and violation records of individuals.

Finally, the EDW must have undergone Vulnerability Assessment and Penetration Testing (VAPT) by a reputable third-party assessor within the last 6 months prior to the publication or posting of this project’s bid documents with the PhilGEPS. The VAPT report as certified by the third-party must indicate that the EDW has no outstanding critical or high vulnerability. Proof of the VAPT must be submitted as part of the Technical Specifications.

c. Digitization of the DSQC’s Clearances and corresponding supporting documents

The service provider must fully digitize about 80,000 pages of clearances and supporting documents. This effort aims to update and clean up the existing database, which has not been updated since the last operation in August 2023.

	Sub-task	Description
1	Grooming	<ul style="list-style-type: none"> • Removing staple wires, fasteners, binders and the like • Smoothen creases on papers • Using acetate cover for documents printed on onion skin or similar delicate paper material • Refastening (in cases of staple wires, clips, etc.) of documents • Grooming task shall be performed onsite
2	Scanning	<ul style="list-style-type: none"> • Scanning the documents using the scanning machine • Document scanning shall have a resolution of 300dpi for colored or black and white • Flat-bed documents shall be used for delicate documents • Scanning of documents will be done onsite • Sizes of the documents to be scanned are not limited to the following: A4, Short, Legal or A3 • Scanned images will be saved using industry standards, such as, TIFF, G4, PDF/A, searchable PDF or the like • Digital Images can be viewed and printed using standard PC and Printer • Uploading of digitized records into a defined storage area
3	Indexing	<ul style="list-style-type: none"> • Indexing shall be conducted offsite in a location identified by the Service Provider
4	Quality Assurance	<ul style="list-style-type: none"> • Checking encoded indices as to 99.95% accuracy and completeness

	(QA)	<ul style="list-style-type: none"> • View and check all scanned images as to clarity, completeness and accuracy vis-à-vis the actual paper documents • Generate report on scanned and processed documents for the day • QA shall be done offsite
5	Transmittal	<ul style="list-style-type: none"> • Upload and transmit the scanned documents into the EDW
6	Storage	<ul style="list-style-type: none"> • Storage of the converted digital documents shall be on the cloud at the designated EDW
7	Web-based User Acceptance Tool	<ul style="list-style-type: none"> • Organize the documents in folders so that reviews can be done in batches • Provide a means to make a list of random samples for review • Present the document images and indexes side-by-side to make the review process easy • Provide a means to navigate from one document to the next • Provide a means for reviewers to tag/identify documents or indexes that must be reprocessed by the Service Provider • Create an audit trail that keeps track of all actions performed on each document • Provide a means to extract data to create reports relating to the review process • Allow reviewers to perform the review process from different locations • Allow reviewers to zoom in/out and rotate the document image within the tool • Supports viewing of both TIFF and PDF formats

d. Manpower Requirements

Depending on the nature of the assignment, the Service Provider shall assign at least five (5) personnel for the Project, and they will report either onsite or remotely. When reporting on-site, employees are expected to adhere to the DSQC's regular business hours. The Service Provider may request to work beyond 8 hours or during weekends or holidays, subject to the prior approval of the DSQC.

e. Maintenance and Technical Support

1	5-hour response time on-site support, 8:00a.m. to 5:00 p.m., Mondays to Fridays. On-next-day support if issue cannot be resolved during working hours.
2	24-hour resolution time and provision of service/replacement units if hardware issue is not resolved within 24 hours.
3	24/7 telephone support/helpdesk facility for initial analysis and resolution of hardware and software related problems.

f. Cloud Platform Subscription Technical Specifications

The cloud platform that will host the Electronic Data Warehouse System shall have the following features, and specifications:

Service Features:

Disaster Recovery and Business Continuity	Plans and processes implemented to ensure that the organization can recover and continue its critical functions in the event of a disaster or disruptive incident.
Automation	To perform tasks with minimal human intervention, which improves efficiency, accuracy, and consistency.
Traffic Management	Techniques and tools employed to monitor, optimize, and control network traffic to ensure efficient data flow, minimize congestion, and enhance overall network performance.
Data Management	The systematic handling of data throughout its lifecycle, including data collection, storage, processing, and retrieval, with a focus on maintaining data quality and security.
Identity Management	The administration and control of user identities and access privileges within an organization's IT infrastructure, ensuring only authorized individuals have appropriate access to resources.
IP Requirement	The identification and allocation of IP (Internet Protocol) addresses to devices on a network, essential for proper communication between devices over the Internet.
Security	Implementation of measures to safeguard an organization's IT systems, networks, and data from unauthorized access, attacks, and other security threats.
Privacy	Protection of individuals' personal information and ensuring compliance with privacy regulations by implementing policies, practices, and technologies that safeguard sensitive data.
Back up capability	The ability to create and maintain copies of critical data to be used for recovery in case of data loss, system failures, or other unforeseen incidents.
Scalable Resources	The ability to handle increased demands by easily adjusting resources such as computing power, storage, and bandwidth.
Software License Requirements	Ensure compliance with legal and contractual obligations related to the acquisition, usage, and distribution of software within an organization.
Period performance	Evaluation and monitoring of system or application performance over specific time intervals to identify trends, issues, and opportunities for improvement.
Support	Providing assistance, troubleshooting, and maintenance services

	to end-users to ensure optimal functionality and address issues promptly.
Knowledge Transfer	The process of sharing and disseminating information, skills, and expertise to ensure continuity and effective utilization of knowledge.

g. Other Hardware and Software Requirements

The Service Provider shall provide all other equipment necessary for the successful implementation of the Project. This may include, but is not limited to, desktop computers, uninterruptible power supply, storage devices, networking equipment and electrical wiring/extension cords. At the expiration of the Project, all other hardware and software requirements provided for by the Service Provider shall be pulled-out from the Project office.

h. Reports

The Service Provider shall submit the following status reports on a regular basis detailing the actions taken to guarantee the upkeep and continuous enhancement of the service:

Risk Level Monitoring Report	Displays the establishments and their corresponding risk level and inspection status
Work Status Monitoring Report	Provides a comprehensive overview of the status and progress of ongoing work of all teams and inspectors
Business Establishment Report	Represents the completeness, compliance, and consistency of a business establishment alongside the classification and/or nature of the business
Worker Productivity Report	Displays the productivity of an inspector based on the status of their assigned workload.
Environmental Inspection Progress Report	Showcases the team's performance by visually presenting trends of improvement.
Timeliness vs Target	Focuses on assessing and comparing the extent to inspections are completed within a specified timeframe in relation to predetermined goals or targets, and the reason for delays or cancellation
Carryovers Status Analysis Report	Provides a concise analysis detailing incomplete inspections, carryover numbers, rate of carryover accumulation, accomplishment percentages, and the aging of pending transactions.
Ordinance Violations Report	Provides an analysis that showcases the number of ordinance violations, frequently affected areas, common types of violations

Prior to the commencement of the service, the parties shall meet to reach an agreement regarding the reporting frequency, updated list of reports, and additional information to be reported, if any.

i. Training

The Service Provider shall provide all necessary trainings for the management and operation of the Environment Inspection System and Electronic Data Warehouse System for selected DSQC personnel on the agreed period by the parties.

j. Data Migration

The Service Provider will deliver the data to the DSQC, and within the agreed timeframe of one (1) month, it shall be temporarily stored in a secure cloud-based repository, which will be made accessible to authorized DSQC personnel for download relating to business profiles, environmental inspections, and on-the-spot violations.

The Service Provider shall also provide the DSQC a comprehensive summary report with migration details.

The data will be structured as follow:

- Inspection Record
 - Reports in a form of PDF, TIFF, or JPG
 - Photos
 - Videos
- Business Profile
 - Machine readable data of permitting documents exported through CSV
 - Soft copies of permitting documents
- Violations
 - Machine readable data of violation records
 - Soft copies of issued EVR
 - Photos
 - Videos
 - Soft copies of Order of Payments

III. SYSTEM OWNERSHIP AND DATA OWNERSHIP

All data captured by the system and data resulting from such software solutions shall remain the property of the City, and the cloud-based storage that contains the data will be turned over to the City when the service agreement expires or terminated. Since the software solution is software-as-a-service, the ownership of the software solutions covered by this Project shall remain with the Service Provider.

The Service Provider shall ensure the timely turnover of raw and processed data to the City, adhering to the specified timeframe of one (1) month for delivery with a retention period of three (3) months, allowing DSQC sufficient time to access and utilize the information effectively.

IV. ENVIRONMENTAL INSPECTION SYSTEM ACCOUNT

The Service Provider shall ensure that the DSQC is the owner of any user account to be utilized for the Environmental Inspection System.

V. REPRESENTATIONS AND WARRANTIES OF THE DSQC

The DSQC shall provide:

- (i) A secure work area complete with tables, chairs, lighting and air-conditioning;
- (ii) Office supplies needed for the Project;
- (iii) Internet connectivity with the recommended bandwidth necessary for the transmission of the final output and submission of the accompanying reports; and
- (iv) The necessary personnel, such as but not limited to a Project Head and/or a Single Point of Contact (SPOC) from the DSQC who will monitor, assist, liaise, coordinate, and represent the department, on any and all matters about the Project.

VI. REPRESENTATIONS AND WARRANTIES OF THE SERVICE PROVIDER

- a. The Service Provider is duly organized and validly existing under and by virtue of Philippine laws and possesses the necessary licenses and permits to conduct its business as currently conducted.
- b. The Service Provider, in the performance of its services, shall secure and maintain at its own expense all registrations, licenses or permits required by national or local laws and shall comply with the rules, regulations and directives of regulatory authorities and commissions. The Service Provider undertakes to pay all fees or charges payable to any instrument of government or to any other duly constituted authority relating to the use or operation or the installation of the equipment and the EDW.
- c. The Service Provider warrants compliance with labor laws, rules, and regulations, including those laws governing employees' compensation and mandatory government contributions, such as PhilHealth, SSS and Pag-IBIG.
- d. The Service Provider warrants that the manpower that shall be assigned to the Project is hardworking, qualified, reliable, and dedicated to doing the service. The Service Provider warrants that it shall assign well-behaved and honest employees with IDs displayed conspicuously while working within the DSQC premises.
- e. The Service Provider's personnel shall take all necessary precautions for the safety of all persons and properties at or near their area of work and shall comply with all the standards and established safety regulations, rules and practices.
- f. The Service Provider shall hold free and harmless the concerned office of the DSQC whose records are to be digitized from any loss, damage or injury due directly or indirectly through the fault or negligence of Service Provider's personnel.
- g. The Service Provider shall neither assign, transfer, pledge, nor subcontract any part of or its interest in the Project.

VII. CONFIDENTIALITY OF INFORMATION AND DATA PRIVACY

- a. The Service Provider shall document detailed procedures/techniques in identifying

system security risks and breaches and how such shall be handled.

- b. All manpower and personnel of the Service Provider shall be required to sign a non-disclosure agreement.
- c. The Service Provider agrees to hold the Confidential Information it obtains by virtue of the Project, in strict confidence. Service Provider furthermore agrees not to copy, reproduce, transcribe, or disclose the Confidential Information to third parties without prior written approval of the DSQC, as the case may be, whose records are to be accessed. For purposes of this provision, "Confidential Information" shall include, but not be limited to the names, addresses and services availed by the person whose record has been accessed. Moreover, where Confidential Information consists of personal information of a data subject (as these terms are defined by the Data Privacy Act of 2012 and its Implementing Rules and Regulations and issuances of the National Privacy Commission (collectively, "the Privacy Laws"), Service Provider shall observe the requirements of the Privacy Laws in the processing of such information.

VIII. MINIMUM QUALIFICATIONS OF THE SERVICE PROVIDER

- a. The Service Provider must have been in the business of information technology or cloud services for at least five (5) years.
- b. The Service Provider must have completed at least one (1) information technology or cloud infrastructure or cloud hosting contracts for the past three (3) years, with a contract price that is at least fifty percent (50%) or equivalent to the Approved Budget of the Contract (ABC) of the Project. Submission of the necessary certifications or its equivalent is required during the post-qualification period.
- c. The Service Provider must have at least two (2) completed information technology or cloud infrastructure government projects with a SATISFACTORY PERFORMANCE or similar rating for the last five years. Submission of the necessary certifications or its equivalent is required during the post-qualification period.
- d. The Service Provider must be registered with the National Privacy Commission (NPC).
- e. The Service Provider must be registered with the Social Security System, Pag-IBIG Fund, and the Philippine Health Insurance Corporation. Proof of registration, or its equivalent, is required during the post-qualification period.
- f. The Service Provider must have a physical office and must have been continuously operating in the said physical office for the past five (5) years. Proof of this is required during the post-qualification period.
- g. The Service Provider must have successfully implemented an environmental inspection system for an environmental and/or sanitation department with a local

government unit for the preceding five (5) years. Submission of the necessary certifications or its equivalent is required during the post-qualification period.

IX. DELIVERY SCHEDULE/DURATION

The Delivery Schedule shall be within thirty (30) days upon the issuance of the Notice to Proceed observing the schedule of delivery as stated below:

MILESTONES	DELIVERY PERIOD
Project Implementation Plan	Within 5 calendar days from the issuance of Notice to proceed
Subscription to the Environmental Inspection System, applications and modules	Within 30 calendar days from the issuance of Notice to Proceed
Subscription to the EDW and Cloud Platform that will host the EDW	Within 30 calendar days from the issuance of Notice to Proceed
Project Support and Maintenance	One year with another 12 months from the end/ termination of the contract

X. APPROVED BUDGET FOR THE CONTRACT

The approved budget for the contract is ten million pesos (P10,000,000.00) inclusive of applicable taxes.

XI. PAYMENT SCHEDULE

10% of the Contract Price	Upon deployment of the Environmental Inspection system apps and modules, cloud platform and the EDW that is approved and accepted by the end user.
90% of the Contract Price – Subscription Fee	In equal monthly payments representing monthly subscription fee for the Environmental Inspection system apps and modules, cloud platform and the EDW that are approved and accepted by the end user.


XII. 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.

XIII. 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 of insolvency, or for cause, it may enter to negotiated procurement pursuant to RA 9184 and its revised IRR.

Prepared by:



ATTY. HANNAH MAE MEDES
CIC Chief, Permits and Compliance Division, DSQC

Reviewed and endorsed by:



PAUL RENE PADILLA
Department Head, Information Technology Development Department

Noted by:



RICHARD SANTUILE
Department Head, DSQC