



TERMS OF REFERENCE (TOR)

SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND TESTING OF NETWORK FIREWALL, COMPUTER ANTIVIRUS SOFTWARE LICENSES, AND DIGITAL ARCHIVING SUPPORT AND SOFTWARE UPGRADE AND CUSTOMIZATIONS FOR THE QUEZON CITY GENERAL HOSPITAL

I. RATIONALE AND BRIEF BACKGROUND

The procurement of network firewall, antivirus software license, and digital archiving support for the Quezon City General Hospital is a critical initiative at enhancing the hospital's cybersecurity infrastructure and digital data management capabilities. Quezon City General Hospital is a public healthcare institution serving a large population in Quezon City, and rely heavily on information technology to manage patient records, administrative data, and communications. However, with the increasing number of cyber threats and the need to comply with data protection regulations, it is imperative for QCGH to invest in robust cybersecurity solutions.

The Quezon City General Hospital also recognizes the importance of supporting the existing Medical-Records Archiving System (MDAS) at Quezon City General Hospital. To achieve this, the organization is undertaking a project to provide dedicated support and manpower to facilitate the efficient operation of the system. The QCGH Medical-Records Archiving System (MDAS) is responsible for storing and managing patient records, medical images, and administrative documents. However, the system requires additional assistance to optimize its functionality and ensure smooth operations. As part of this project, the Quezon City General Hospital will allocate trained personnel to work closely with QCGH staff, helping them navigate and utilize the Medical Records Archiving System effectively. These dedicated professionals will provide hands-on support, assisting users in retrieving, uploading, and organizing digital records, ensuring accurate and secure data management.

The key component of this project includes:

1. **Network Firewall** to protect QCGH's internal network from unauthorized access, malware, ransomware, and other cyber threats. It will act as a barrier between the hospital's internal systems and external networks, ensuring data security and network integrity.
2. **Antivirus Software** for real-time detection and prevention of malware, viruses, and other malicious software. It will help safeguard the hospital's computer systems and data from potential threats that could disrupt operations or compromise sensitive patient information.
3. **Digital Archiving Support and Software Upgrade and Customizations** involves personnel that will collaborate with QCGH medical records users, addressing any challenges, resolving technical issues, and providing training sessions to promote user proficiency and confidence. This support shall also include software upgrade, enhancements, and customizations. Manage QCGH users to navigate the system seamlessly, ensuring swift access to patient information, reducing administrative burdens, and optimizing the overall workflow within the hospital.



The successful implementation of these components will contribute to the following:

- Improved data security: Protecting sensitive patient information and ensuring compliance with data protection regulations.
- Enhanced network resilience: Safeguarding the hospital's network infrastructure against cyberattacks and potential disruptions.
- Efficient data management: Streamlining the storage, retrieval, and management of digital records and documents, ultimately improving administrative processes and patient care.

This initiative underscores the hospital's commitment to providing quality healthcare services while safeguarding patient information and maintaining operational efficiency in the face of the evolving digital landscape and cybersecurity challenges.

II. PROJECT DESCRIPTION

This project entails the provision of managed services for digital archiving support at Quezon City General Hospital. The key components of the project are as follows:

1. Supply, Delivery, Installation, Configuration, and Testing of Antivirus Software:

- A total of **171** units of antivirus software will be supplied, delivered, and installed across various departments and offices within Quezon City General Hospital.
- These antivirus software units will be configured to ensure optimal protection against digital threats.
- Rigorous testing will be conducted to verify the effectiveness of the antivirus software.

2. Deployment and Configuration of Network Firewall:

- One unit of a management appliance will be deployed in the hospital's IT server room.
- A one-year subscription of network firewall services will be included in this management appliance.
- The network firewall will be configured to enhance the security and integrity of the hospital's digital infrastructure.
- Included training or seminar to I.T. Personnel with certificate.

The project aims to safeguard the hospital's digital assets and data by implementing comprehensive security measures. The deployment and configuration of these software and hardware solutions will be executed to the highest standards to ensure the hospital's digital environment remains secure and resilient.



III. PROJECT SCOPE OF WORK

The project shall cover the delivery of services for the installation, configuration, testing, deployment, documentation, and implementation of Network firewall, antivirus software and digital archiving support which includes but not limited to the following:

- Project Management
 - a. Project Plan
 - b. Installation and Configuration of Network Firewall and Antivirus software
- Project Documentation
- Warranty and Support Services 1 year coverage after full acceptance of project

(LINE 1) HARDWARE / SOFTWARE SPECIFICATIONS

- a. Network Firewall Appliance (1 Unit)

Minimum Technical Specifications	
Mounting	1U rackmount
Power supply	Internal auto-ranging DC 100-240VAC, 3-6A@50-60 Hz External Redundant PSU Option
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC* , KC, BSMI* , RCM, NOM, Anatel
Performance	
Firewall throughput	40,000 Mbps
Firewall IMIX	24,500 Mbps
Firewall Latency (64 byte UDP)	4 μs
IPS throughput	13,440 Mbps
Threat Protection throughput	2,770 Mbps
Concurrent connections	13,700,000
New connections/sec	257,800
IPsec VPN throughput	6,500 Mbps
SSL/TLS Inspection	3,130 Mbps
SSL/TLS Concurrent connections	102,400
Features	<ul style="list-style-type: none">• TLS 1.3 inspection• Next-Gen Intrusion Prevention (IPS)• Zero-day threat protection• Proxy-based dual-engine AV scanning• Perimeter defenses• Country-based blocking policy• Hardware acceleration• Intelligent traffic selection• Pre-packaged exception list• Powerful policy engine• Covers all ports/protocols• Supports all modern cypher suites• Unmatched visibility and error handling• Advanced Web Protection• Pharming protection



	<ul style="list-style-type: none">• HTTPS scanning• Potentially unwanted app control• Security Heartbeat• Active Threat Response• Lateral Movement Protection• Destination Heartbeat Protection• Synchronized App Control• Synchronized User ID• Multiple threat feeds supported.• Blocks active threats immediately without the need for firewall rules• Utilizes Synchronized Security to automatically isolate managed endpoints and provide visibility• User identity powers all firewall policies and reporting• User Threat Quotient (UTQ) identifies the top risk users on your network• Synchronized User ID• Flexible authentication options including directory services• Two-factor Authentication (2FA) one-time password support for Access to key system areas• Visibility and control over thousands of applications• CASB cloud app visibility• Generative AI Visibility and Control• Synchronized App Control• User-based application policies• Traffic shaping (QoS) prioritizes bandwidth allocation to critical applications and limits bandwidth for non-business applications• Enterprise Secure Web Gateway (SWG) policy model• Support for DNS Protection• Template-driven activity control with predefined workplace and compliance policies• Education and SafeSearch features• Comprehensive traffic enforcement• Traffic shaping (QoS)• Web keyword monitoring• File download filtering templates• Policy-based outbound email DLP• Web caching• Next-generation IPS• Web Application Firewall• Granular, user-based protection
--	---



	<ul style="list-style-type: none">• Full MTA store and forward support• Live anti-spam• SPX encryption• Policy-based DLP• Self-serve user portal
--	--

(LINE 2) Computer Software

- A.Digital Archiving Support and Software Upgrade and Customizations
- Management and Maintenance of Digital Records and Archives
 - Software Upgrade and Enhancements
 - Implement customized modules for all departments.
 - Upgrade software to its latest version.
 - Performance optimizations
 - Improve overall system functionalities.
 - User interface improvements
 - Reports and Dashboards improvements
 - Weekly, Monthly, Quarterly and Yearly system reports (output)
 - Technical Support to QCGH Medical Records Archiving System (MDAS)
 - Training and Guidance to QCGH MDAS users for digital archiving best practices for efficient utilization of the system.
 - Software System and Database backup
 - Security patches updates
 - Documentation, Training Modules and Training

DIGITAL ARCHIVING SUPPORT AND SOFTWARE UPGRADE AND CUSTOMIZATIONS

Qualified personnel specializing in digital archiving support will be stationed within the Information Technology department. Their responsibilities will include:

1. *Management and Maintenance:* Overseeing the organization and preservation of digital records and archives within the hospital's IT infrastructure.
 - Crafting comprehensive policies and procedures for digital recordkeeping, ensuring they align with legal requirements and industry standards. This includes establishing guidelines for record creation, classification, retention, and deletion.
 - Regularly evaluating and optimizing the digital archiving system's performance. This includes ensuring the integrity of digital records, conducting periodic audits, and updating the archiving system to incorporate the latest technological advancements.
 - Implementing robust digital preservation strategies to safeguard records against technological obsolescence and ensuring long-term accessibility. This may involve format migration, emulation, and employing redundancy techniques to prevent data loss.
2. *Software Upgrade, Enhancements and Customizations of QCGH Medical Records Archiving System (MDAS)*
 - Upgrades and Enhancements
 - **Additional Module for all departments** - Each department will have their own module in the Medical Records Archiving System (MDAS) to facilitate their archiving of documents in the system.

Each department will set their preferred information / data to be used for indexing.

- **Performance** - Process improvements will be taken to optimize system performance, ensuring faster response times and efficient resource utilization.
- **Feature Functionalities** - Enhancements will be made to feature functionalities, addressing user needs and incorporating additional capabilities to improve overall system functionality.
- **Dashboards and Reports** - Develop dashboards that provide real-time insights into archived records, system usage, and performance metrics. Generate custom reports based on specific data points, facilitating better decision-making and operational efficiency.
- **Weekly, Monthly, Quarterly and Yearly system reports** – Output required by the hospital.
- **System and Database Backup**
 - Daily backups shall be performed to capture changes and updates made to the system each day. Daily backups will be scheduled during off-peak hours to minimize any potential impact on system performance and user experience.
 - Weekly full backups shall be conducted to create comprehensive snapshots of the entire system. Weekly full backups will be scheduled during a specified maintenance window to ensure minimal disruption to regular operations.
 - External Backup Storage - To enhance data redundancy and disaster recovery capabilities, external backups will be stored in the backup server of the Civil Registry. This external backup storage serves as an additional layer of protection, ensuring that critical data is securely preserved in a separate location.
- **Security**
 - The server should have up-to-date antivirus and anti-malware measures with updated security software to detect and mitigate the risk of viruses or malicious software that could compromise the system's integrity.
 - The server should only enable necessary ports and ensure that they are secured. Restrict access to ports that are not essential for the application's functionality. Implement firewalls and access controls to prevent unauthorized access through open ports.
 - The service provider must conduct a thorough Vulnerability Assessment and Penetration Testing (VAPT) process to identify and address potential vulnerabilities in the system. This testing will include both automated scanning tools and manual testing to ensure the robustness of the security measures.

3. *Technical Support:* Providing assistance, troubleshooting, and expertise in managing and accessing archived digital data.

- Addressing technical issues that arise during the storage, retrieval, or management of digital archives. This includes solving problems related to data corruption, access rights, and system malfunctions.
 - Designing and implementing customized solutions to meet specific departmental needs for accessing and using archived information, enhancing operational efficiency across the hospital.
 - Ensuring the security of digital archives by implementing strong access controls, encryption, and monitoring systems to protect sensitive information from unauthorized access or cyber threats.
4. *Training and Guidance:* Offering guidance and training to hospital staff regarding digital archiving best practices to ensure efficient utilization of archived data.
- Conducting workshops and seminars to educate hospital staff about the importance of digital archiving, the correct procedures for document digitization, and the nuances of data retrieval.
 - Developing and disseminating best practice guidelines to all departments, emphasizing the critical role of proper documentation and archiving in maintaining high standards of care and compliance.
 - Encouraging a culture of continuous learning and adaptation among hospital staff regarding digital archiving, incorporating feedback into training programs to address evolving challenges and technological advancements.

B. Computer Antivirus Software (171 units)

- Antivirus Software Licenses
- Training to QCGH Applicable Users for Antivirus Software and Management
- Technical Support for Computer Antivirus Software and Management
- Features
 - a. Real-Time Antivirus
 - b. Online Payment Protection
 - c. Performance Optimization
 - d. Unlimited Superfast VPN
 - e. Data Leak Checker
 - f. Identity Protection
 - g. Expert Virus Check & Removal
 - h. Hard Disk Cleaner & Health Monitor
 - i. Anti-Hacking
 - j. Existing Threat Removal
 - k. Anti-Ransomware

Managed services:

- a. Project Management
 - i. Project Kick off
 - ii. Qualified Project Manager and PM Team
 - iii. Full Documentation on Project implementation
- b. Warranty, Maintenance and Support
 - 1. Two (2) hours response time for critical issues/Priority
 - 2. 1 year coverage after full acceptance of project



IV. AREA OF COVERAGE

The deployment of the network firewall and antivirus software will encompass all computers within Quezon City General Hospital. These security measures will be applied uniformly across all departments and offices to ensure comprehensive protection against digital threats.

V. PROJECT STANDARD 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 SEC or DTI 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 must have implemented and completed an implementation of Network Firewall and Antivirus Software within the last three (3) years.
- d. The service provider must have implemented and completed a digital archiving project within the last three (3) years.
- e. 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 provider must have a Platinum status in PhilGEPS.
- b. The service provider must be a duly registered company with SEC or DTI filing.
- c. The service provider must be duly registered under 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

The contractor/Service Provider/Bidder shall have the critical technical knowledge that includes knowledge of database systems; ability to manage database system integration, implementation, and testing; ability to manage relational databases and create complex reports; knowledge and ability to implement data and information policies, security requirements; and knowledge of client tools used by business users. The project should provide the following Professional Services:



- a. Project Manager (1) - The Project Manager should have at least experience in digital archiving system, network security system implementation.
- b. Programmer (1) - Programmer will develop and customize the system upgrade and customizations requirements for MDAS.
- c. Web Security Engineer (1) - Will focus on safeguarding the system from security threats, conducting assessments, implementing security protocols, and ensuring compliance.
- d. Quality Assurance and Testing Staff (1) - Responsible for ensuring the overall quality of system through test planning, execution, defect identification, and collaboration with the development team.
- e. Network Administrator (1) – Network Administrators are for the installation and configuration of network firewall and antivirus software. This administrator will provide support systems to assure continuous operation of the firewall and antivirus software.
- f. Technical Support (1) - The Technical Support is responsible for providing technical assistance and troubleshooting for both the network firewall and antivirus software. This support ensures that any technical issues are promptly addressed, and system users receive the necessary assistance to resolve problems and optimize system performance.
- g. Digitization Expert (2) – The Digitization Expert will be the assigned support for the digital archiving of QCGH and will collaborate with QCGH users, addressing any challenges, resolving technical issues, and providing training sessions to promote user proficiency and confidence. This support shall also manage QCGH users to navigate the system seamlessly, ensuring swift access to patient information, reducing administrative burdens, and optimizing the overall workflow within the hospital.

VI. TRAININGS

The service provider will provide necessary trainings to all IT personnel of QCGH with four (4) hours training duration. A separate training for medical records for the digital archiving support and management to be conducted by a digitization expert with an equivalent of four (4) hours training.



VII. AFTER SALES SUPPORT

The service provider will submit an Affidavit of Undertaking stating the following:

- Software Component will have one (1) year warranty upon implementation.
- User manual and installer will be provided for software components.
- All hardware components will have one (1) year warranty upon delivery and configuration.
- Technical Support:
 - Workdays from 8AM to 5PM, expect a response within the day or by next day.
 - Weekends and holidays, expect a response by next workday.

VIII. DELIVERY SCHEDULE

Sixty (60) calendar days delivery period.

The project duration shall be one (1) year upon issuance of the Notice to Proceed observing the schedule of delivery as stated below:

MILESTONES	DELIVERY PERIOD
Delivery of Hardware	Within calendar 30 days upon issuance of the Notice to Proceed
Installation and Configuration of Network Firewall and Antivirus Software	Within 60 days upon receipt/issuance of the Notice to Proceed
Training and Turnover	7 calendar days upon completion of installation and configuration of Network firewall and antivirus software.
Project Support and Maintenance	One (1) year upon project completion and acceptance.



IX. BASIS FOR PAYMENT

The terms of payment shall be based on the following completed deliverables:

- a. Upon submission of the delivery of the Project Management Plan, the procuring entity will release fifteen percent (15%) of the total winning bid amount to the service provider.
- b. Upon completion of delivery of Hardware IT equipment, completion of configuration and setup. The procuring entity will release twenty three percent (23%) of the total winning bid amount to the service provider.
- c. Upon deployment of the network firewall and antivirus software, the procuring entity will release sixty one percent (61%) of the total winning bid amount to the service provider, including the following:
 - Installation and Configuration of Network Firewall and Antivirus software
 - Knowledge Transfer/ Training
- d. One percent (1%) of the total winning bid amount will be released one (1) year after the final acceptance of the system as performance security.

X. APPROVED BUDGET FOR THE CONTRACT

The Approved Budget for the Contract (ABC) amounts to **Seven Million Nine Hundred Seven Thousand Five Hundred Seventy-Five Pesos. (Php7,907,575.00)**



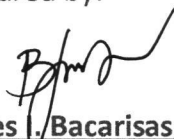
XI. PENALTIES FOR BREACH OF CONTRACT

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.

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.


Prepared by:


James L. Bacarisas, MMPA

Information Systems Analyst III

OIC, QCGH-Management Information System Section

Approved by:


Josephine B. Sabando, MD, RN, FPBA, MHA, FPSA
Medical Center Chief II
Hospital Director