CyberSecurity MALAYSIA

SEBUTHARGA NO.: SH/28/2022
SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
A	**GENERAL REQUIREMENTS**				
1.0	**SCOPE OF WORKS**				
1.1	The bidder **MUST** fully comply with the scope of works, which includes the supply, delivery, testing, commissioning, handover, and acceptance of the system specified in the Bill of Quantities and Price Schedules (BQ).	M			
1.2	The system shall be delivered to CyberSecurity Malaysia, Selangor, Malaysia.	M			
1.3	The system shall be installed, tested, and endorsed by CyberSecurity Malaysia upon completion of the User Acceptance Test (UAT).	M			
1.4	The bidder shall confirm that their proposal is based on the entire provision of the above scope of works. The bidder's partial compliance to the said scope of works shall be disqualified.	M			
2.0	**BIDDER'S RESPONSIBILITY**				
2.1	The bidder shall review this document and take full responsibility for obtaining information from CyberSecurity Malaysia as may be required to meet the specifications and requirements.	I			
2.2	The bidder shall review and fulfill all specifications and requirements before committing to sign the purchase agreement.	M			
2.3	The bidder **MUST** provide a complete proposal for the system.	M			
3.0	**BIDDER PAST EXPERIENCES**				
3.1	Bidder shall possess a minimum of two (2) years of similar experience for this provision.	M			
3.2	Bidder to provide a list of past clients for CyberSecurity Malaysia's reference.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only: These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

SEBUTHARGA NO.: SH/28/2022
SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
4.0	**DOCUMENTATION REQUIREMENTS**				
4.1	All documentation shall be in English. The bidder shall be responsible for any translation cost incurred (if any) in regard to the submission of the documentation required by this tender.	M			
4.2	CyberSecurity Malaysia reserves the right to reproduce all or part of the document submitted by the bidder for internal use.	G			
4.3	Bidder to provide brochures and other relevant documentation for the system.	M			
5.0	**WARRANTY REQUIREMENTS**				
5.1	The warranty of the system **MUST** be six (6) months standard warranty and services from the commissioning date and acceptance by CyberSecurity Malaysia.	M			
5.2	Maintenance and support services for the system shall also be for a duration of six (6) months upon completion.	M			
5.3	The bidder is to provide the details on the remedial and/or preventive maintenance schedule during the warranty in the proposal if such maintenance offers by the vendor.	M			
5.4	The warranty shall include labor.	M			
5.5	The bidder must provide six (6) months support and maintenance including: • 8 x 5 x next business day on-site support • Onsite support • Phone, email, helpdesk support • Preventive maintenance	M			
5.6	The bidder **MUST** provide at least one phone number with 24 hours X 7 days that will cover by email and helpdesk support. Any problem reported via email should be responded to by a helpdesk/ticketing system with a unique case ID number.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only: These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

SEBUTHARGA NO.: SH/28/2022

SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
6.0	**DELIVERY REQUIREMENTS**				
6.1	The successful bidder shall complete the entire scope of works in twelve (12) weeks or earlier after receipt of the CyberSecurity Malaysia's Letter of Acceptance (LOA).	M			
6.2	CyberSecurity Malaysia has the right to reject any kind of bugs during or after installation (within the warranty period). The replacement shall be done within the same day without extra charge	M			
6.3	The bidder shall ensure to conduct, assist, and deliver any services related to enhancing the security aspects of the system including Pentest.	M			
6.4	Upon completion of the development works, the bidder is required to submit: i) User Acceptance Test report. ii) Testing and/or assessment report. iii) Source code iv) Final report.	M M			
6.5	All documents, reports, or materials prepared or developed by the vendor specifically in relation to or for the purpose of this Proposal, shall unless otherwise expressly agreed, belong to CyberSecurity Malaysia.	M			
6.7	Once the party agreed to the terms of the system or dashboard, a separate term will be negotiated between the parties for the development, then the source code shall be transferred to CyberSecurity Malaysia once payment has been made.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -

M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.

G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.

I – For Info Only: These are information for the Bidder to take note and acknowledge.

Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

SEBUTHARGA NO.: SH/28/2022
SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
B.	**TECHNICAL SPECIFICATIONS & REQUIREMENTS**				
1.0	**PURPOSE** To deploy, install, configure, integrate, test, hand over and acceptance of the PGPKS Dashboard System for CyberSecurity Malaysia.	I			
2.0	**TECHNICAL SPECIFICATION** Bidder's proposal for the development of the PGPKS Dashboard System **MUST** be able to follow the following specification and features or equivalent or higher: -	I			
2.1	The technology stack for this project opened as follows: - • ASP.NET Blazor on .NET 6 • HTML, CSS, JavaScript • ASP.NET on .NET 6 based on C# • Portal Data Repository / Source • PHP 8 • Laravel 8 Framework • Javascript and JQuery • CSS Bootstrap 5 Framework • MySQL / MariaDB Database • Apache Web Server 2.4 or latest	M			
2.2	The implementation of the scope of work is to develop the groundwork for the PGPKS Dashboard System including the components as below:	M			
2.2.1	**Portal Landing Page** To construct and develop a public-facing landing page with agreed UI/UX design and content to be provided by business users	M			
2.2.2	**Authentication and Authorization** To develop and integrate an authentication and authorization module with access control management functionality on the portal	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only: These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

SEBUTHARGA NO.: SH/28/2022
SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
2.2.3	**Dashboard Portal** To develop following dashboards to display and showcase protected content and infographic based on authenticated user's role. • Overall Program dashboard – PGPKS Scoring for external view • Health check dashboard • Registration dashboard • PMO dashboard	M			
2.2.4	**Data Upload / Import** To develop a Data upload / Import functionality to capture and store data collected from various information source provides. Namely, Health Checks, VAPT, Risk Assessment Data Upload is controlled by system. assigned batch number, and application users can disable the entire batch data and re-upload new / corrected data in the event of data modification and correction.	M			
2.3	This developed Dashboard system will include several modules includes: • User Type • Administrator • Data Entry • SME Companies or Client • Management	M			
2.3.1	**User Access Module** The User Access module covers the basics of controlling applications access to the developed system. It includes the following features: • Login • Log out • Forgot password • Registration • Profile page • Update profile • Change Password	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only: These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

SEBUTHARGA NO.: SH/28/2022
SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
2.3.2	**User Management Module** Administrator users have access to modules for management users with the following functions: • Creating a new user • Set the user type • Updating user data • Prevents access to users	M			
2.3.3	**Dashboard module** • The Dashboard module is a module for users to access • Management. • The dashboard has one page with several widgets • displays the latest status on the development of the PGPKS program. • Widgets in the Dashboard can be clicked to display one or more information if any.	M			
2.3.4	**Data Management Module** • The Data Management module is used by Data Manager users. • The Data Manager can have access to the following functions: o Enter SME Company information o Updating SME Company information o Update the latest score status of SME Companies o Updates data for existing widgets in the Dashboard	M			
2.3.5	**Program Formulation Module for SMEs** This module is for access by Private Companies (SMEs) for review of their company summary in the PGPKS program.	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only: These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

SEBUTHARGA NO.: SH/28/2022
SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL	PLEASE TICK IF BIDDER COMPLY	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
2.4	**USER ACCEPTANCE TEST**				
2.4.1	The project involves the following two (2) user testing activities: • User Acceptance Test (UAT) - twice • Final Acceptance Test (FAT) - one time	M			
2.4.2	The bidder will also provide a test script and test plan for • implementation of UAT & FAT. • Preparation for UAT & FAT	M			
2.4.3	CyberSecurity Malaysia will arrange the venue and hardware.	I			
2.5	**TRAINING**				
2.5.1	The bidder will conduct one 2-days training session for 2 pax.	M			
2.5.2	The bidder will provide manuals and other necessary documents for a training session.	M			
2.5.3	The bidder will provide coaches for training sessions.	M			
2.5.4	CyberSecurity Malaysia will provide venue, hardware, food and drinks, accommodation etc. for the implementation of training.	I			
2.6	**DEVELOPMENT INFRASTRUCTURE**				
	The bidder to setup and configure development environment for internal testing and debugging at CSM's data center.	M			

-END OF DOCUMENT-

Note 1 : CyberSecurity Malaysia's Requirement Level: -
M – Mandatory Requirement: These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement: These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only: These are information for the Bidder to take note and acknowledge.
Note 2 : A blank (ie. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.