****

# APPENDIX D -PRODUCT/SERVICE REQUIREMENTS

**WSIPC RFP 23-02 Enterprise Cybersecurity & Risk Assessment Solutions**

## INSTRUCTIONS

Please answer each requirement based on the proposed solution’s ability to satisfy the respective requirement. If the requirement cannot be met and warrants further explanation, a brief explanation may be provided in the “Comments” column. The following scoring system should be used to evaluate each business requirement:

|  |  |
| --- | --- |
| **Response Code** | **Definition** |
| Y—Yes | Requirement is met. |
| N—No | Requirement is not met. |
| Q—Qualifier | Ability to meet requirement requires further explanation from Vendor. Please use the "Comment" column to provide more details. |

## General

| **Requirements/Specifications** | **Yes** | **No** | **Q** | **Comment *(Required if “Q” is selected)*** |
| --- | --- | --- | --- | --- |
| **Product/Service Usage -** The product and/or service is used by other Washington State K-12 school districts and has an active Washington State user community. | [ ]  | [ ]  | [ ]  |       |
| **Documentation -** Describe access to operational, instructional, and/or specification sheets. It is highly desirable that this type of information be available to customers electronically via the internet (preferred) or other electronic means of delivery. | [ ]  | [ ]  | [ ]  |       |
| **Shipping Costs -** All costs for shipping to the buyer’s location, must be clearly stated on price lists and promotional materials, and must be clearly described in the Proposer’s response to this RFP. | [ ]  | [ ]  | [ ]  |       |
| **Vendor Website -** The Proposer must have an active website with published product and/or service information. | [ ]  | [ ]  | [ ]  |       |

## Technical/functional Requirements

| **Requirements/Specifications** | **Yes** | **No** | **Q** | **Explanation *(Required if “Q” is selected)*** |
| --- | --- | --- | --- | --- |
| Multi-feature solution for identifying and addressing threats. | [ ]  | [ ]  | [ ]  |       |
| Robust monitoring functions that operate within existing infrastructure. | [ ]  | [ ]  | [ ]  |       |
| Ability to conduct a thorough risk assessment. | [ ]  | [ ]  | [ ]  |       |
| Ability to design and implement a robust cyber defense model. | [ ]  | [ ]  | [ ]  |       |
| Ability to identify and address malicious code within systems, infrastructure, and applications. | [ ]  | [ ]  | [ ]  |       |
| All tools in regulatory compliance with protecting confidentiality, privacy, integrity, and availability of critical data and systems. | [ ]  | [ ]  | [ ]  |       |
| Identify gaps or vulnerabilities in current security controls and policies and make recommendations and necessary adjustments to correct them. | [ ]  | [ ]  | [ ]  |       |
| Develop comprehensive security policies based on CIS Controls (Center for Internet Security), industry standards, and best practices. | [ ]  | [ ]  | [ ]  |       |
| Facilitate in implementing security policies, software, hardware, and CIS Controls which can serve as foundation for informed decision-making and increased security awareness. | [ ]  | [ ]  | [ ]  |       |
| Offer vulnerability assessments and penetration testing to identify and validate configuration and/or testing flaws within a given system or network (e.g., firewalls, routers, servers, operating systems, applications, databases, etc.). | [ ]  | [ ]  | [ ]  |       |
| Provide security monitoring and defense including unauthorized behavior, malicious hacks, denial of service, anomalies, and trend analysis. | [ ]  | [ ]  | [ ]  |       |
| Provide security operations support including detection, alerting, and possible response. | [ ]  | [ ]  | [ ]  |       |
| Provide incident management and ensure business continuity and disaster recovery. | [ ]  | [ ]  | [ ]  |       |
| Offer digital forensics: ability to investigate security incidents and offer solutions to mitigate future incidents. | [ ]  | [ ]  | [ ]  |       |
| Provide multi-purpose archiving, storage, and replication of data from email and files. | [ ]  | [ ]  | [ ]  |       |
| Provide tools for backup and disaster recovery as well as compliance and e-discovery. | [ ]  | [ ]  | [ ]  |       |
| Advanced Bot Management with essential anti-bot functions that can detect bot activity and stop them. | [ ]  | [ ]  | [ ]  |       |
| Tools that counter advanced bot deployment strategies. | [ ]  | [ ]  | [ ]  |       |
| Ability to fully manage (remotely) cybersecurity infrastructure. | [ ]  | [ ]  | [ ]  |       |
| Robust customer support infrastructure. | [ ]  | [ ]  | [ ]  |       |
| Offer end-user training and knowledge transfer. | [ ]  | [ ]  | [ ]  |       |