التاريخ: 28/11/2022

رقم الاستدراج: Q70-2023

السادة: .....

تلفون: .....

إيميل: .....

استدراج عروض أسعار: الرجاء تزويدنا بأسعار اللوازم التالية شامل لضريبة القيمة المضافة:

	اسم الصنف	الوحدة	الكمية	السعر	اجمالي تكلفة البند
1	Vulnerability Management Systems	عدد	1		
		المجموع الكلي (ش.ض)		USD	

تعليمات الاستدراج		ختم وتوقيع المورد:
** آخر موعد لتسليم العروض هو يوم:	الاثنين	
** الموافق:	05/12/2022	
** طبيعة البنود المطلوبة:	برامج حماية	
** بعملة:	USD	
** الأسعار تشمل التوصيل ل:	الحرم الجامعي-جنين	
** نوع التوريد:	توريد كامل	
** يرجى إرسال العرض ب:	بالظرف المغلق	

شروط الاستدراج:

** ضرورة تحديد مدة الكفالة إن وجدت.

** ضرورة تحديد مدة التوريد من تاريخ استلام امر الشراء، و في حال عدم الالتزام يتم فرض غرامة تأخير .

** ختم وتوقيع المورد المعتمد على هذا النموذج، وكتابة رقم الاستدراج واسم الشركة كما هو مسجل لدى الضريبة على الظرف.

** للمراجعة والاستفسار بخصوص المواصفات يرجى الاتصال على هاتف 042418888 رقم داخلي 1488

** للمراجعة والاستفسار بخصوص المواصفات عن طريق فاكس 042510972 أو بريد الكتروني samah.zaidalkelani@aaup.edu

** لمشاهدة العطاءات والاستدراجات، يرجى الدخول الى الرابط http://www.aaup.edu/tenders

مدير دائرة اللوازم و المشتريات
أ. حسن ربابعة
دائرة اللوازم والمشتريات
PROCUREMENT AND PURCHASING DEPARTMENT

Request for Quotation (RFQ)
Vulnerability Management Systems

Table of Contents

General Terms & Conditions

1. The Bidder, Vendor or OEM Solution must possess all the required specifications mentioned in Part 'Mandatory Requirements'.
2. The Bidder, Vendor or OEM should not be currently blacklisted by any Govt. dept. /Public Sector Unit.
3. The Bidder, Vendor or OEM must be Gartner's quadrant, Forrester, NSS Labs, or any equivalent Test report & certifications.
4. The Bidder, Vendor or OEM should be in the 5. Gartner Magic Quadrant and Forrester for last 3 years.
5. The Bidder, Vendor or OEM should have deployed similar type of solution within the last 2 years in Palestine.
6. The Bidder, Vendor or OEM must have support office in Palestine.
7. Bidder, Vendor or OEM must be able to provide a Presentation and POC on request.

Vulnerability Management Systems

AAUP want to appoint a suitable vendor/Service Provider for Vulnerability Assessment and Penetration Testing (VAPT) of hosted internet facing application servers and firewall.

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface."

Project Scope

VAPT Activities:

VAPT should be comprehensive but not limited to following activities: Network Scanning, Port scanning, system identification and trusted system scanning, Vulnerability scanning, Malware scanning, Spoofing, Application Security Testing, Access Control Mapping, Denial of Service Attack (DOS), Password cracking, Cookie Security, Functional Validations, DMZ Network architecture review, Firewall rule review, OS Security configuration, Database Security Configuration, any other attacks.

Website / Web – Application Assessment:

Website / Web- Application assessment should be done as per the latest OWASP guidelines including but not limited to the following: Vulnerabilities to SQL Injections, CRLF injections, Directory Traversal, Authentication hacking/attacks, Password strength on authentication pages, Scan Java Script for security vulnerabilities, File inclusion attacks, Exploitable hacking vulnerable, Web server information security, HTTP Injection, Phishing a website, Buffer Overflows, Invalid Inputs, Insecure Storage etc. Any Other attacks, which are vulnerability to the website and web-applications. Web Assessment should be done by using Industry Standards and also as per the Open Web Application Security Project (OWASP) methodology to Identify the security vulnerabilities including top web application vulnerabilities viz. Cross Site Scripting (XSS), Injection Flaws, Malicious File Execution, Insecure Direct Object Reference, Cross Site Request Forgery (CSRF), Information Leakage and Improper Error Handling, Broken Authentication and Session Management, Insecure Cryptographic Storage, Insecure Communications, Failure to Restrict URL Access, etc and also to identify remedial solutions and recommendations for making the web applications secure.

The selected Bidder has to undertake VAPT in a phased manner as described below:

PHASE I: Conduct of VAPT as per Scope, Evaluation & Submission of Preliminary Reports of Findings and Discussion on the Findings.

- Conduct of VAPT as per the scope:
    1. AAUP IT Team will call upon the selected bidder, on placement of the order, to carry out demonstration and/or walk-through, and/or presentation and demonstration of all or specific aspects of the VAPT activity at AAUP campus. All the expenses for the above will be borne by the concerned bidder.
    2. VAPT schedule to be provided 7 working days prior to the start of activity along with the team member details. A dedicated Project Manager shall be nominated, who will be the single point of contact for VAPT Activities. The selected Bidder to ensure that

only certified and experienced professionals should be deployed for carrying out VAPT during the audit period.

3. Execute Vulnerability Assessment and Penetration testing of AAUP IT Infrastructure as per the scope on the written permission/Order from AAUP and in the presence of IT Team Officials.
4. Analysis of the findings and Guidance for Resolution of the same.

- Detailing the Security Gaps
  1. Document the security gaps i.e. vulnerability, security flaws, loopholes, threats, etc. observed during the course of the VAPT activity for all AAUP IT Infrastructure as per the scope of work.
  2. Document recommendations and solutions for addressing these security gaps and categorize the identified security gaps based on their criticality, resource/effort requirement to address them.
  3. Chart a roadmap for AAUP to ensure compliance and address these security gaps.
- Addressing the Security Gaps
  1. Recommend fixes for systems vulnerabilities in design or otherwise for application systems and network infrastructure. If recommendations for Risk Mitigation / Removal could not be implemented as suggested, alternate solutions to be provided.
  2. Suggest changes/modifications in the Security Policies and Security Architecture including Network and Applications of AAUP to address the same.

PHASE II: Reporting Submission and Acceptance.

Submission of Reports:

The selected bidder should submit the report of VAPT findings as per the report format. All the VAPT reports submitted should be signed by technically qualified persons and he/she should take ownership of document and he/she is responsible and accountable for the document/report submitted to AAUP IT Team.

Acceptance of the Report:

On receipt of the report from the selected Bidder, AAUP Team will scrutinize and after satisfying about the completeness of the report, AAUP will accept the report. If there are any inconsistencies in the report the selected Bidder should conduct proper test and resubmit the report to AAUP without any additional cost.

IT-Infra in Scope and location:

AAUP IT Team will provide selected Bidder with list of all assets and IT-Infra related to the test, and AAUP expect Bidder to submit accurate questioner to guide AAUP team with the best way to go through VAPT process for best results.

Mandatory Requirements

- Bidder, Vendor or OEM will be fully responsible for Implementation, Configuration, Installation and tanning of Cloud Email Security Gateway.
- Bidder, Vendor or OEM official in-person tanning for at least 2 employees is a must.
- Ongoing Support: Bidders must disclose detailed information confirming the warranty period, replacement strategy of faulty parts, spare parts stock status and length of repair period. Bidders should have sufficient workforce and equipment to provide quality service.
  Detailed System/Equipment Requirements and Technical Architecture:
  Technical Specifications –
    - The bidder should clearly specify and state the methodology, architecture, and design to implement the primary site along with the integration with the current email infrastructure.
    - The entire schedule, with specific milestones must also be presented.
    - Solution Architecture Design.
    - Implementation methodology along with Node and connectivity details.
    - Issue, Suggestion & Risks.
    - Project time schedule & dependency.
    - Integration & Acceptance Test.
- After the installation is complete, Bidders are required to carry out a complete series of commissioning and acceptance tests (POC) for the complete solution with documentation.
- The acceptance tests (POC) shall be carried out to demonstrate the capacity and effectiveness of each feature installed.
- Provide all document and materials which may be required to test (POC) the solution provided.

- Solution should protect against common threats against latest Email Security Risks in 2022
    1- Spoofing and Phishing
    2- Vulnerabilities in E-mail Security
    3- Domain's squatting
    4-Client-Side Attacks
    5-Dangerous Files
    6-Crypto-ransomware
    7- Configuration Errors
    8- Browser Exploit Kit
    9- Spear Phishing attacks and Business E-mail Compromise (BEC)
    10-File Format Exploits.
- All currency in the proposal shall be quoted in $ USD Dollars and prices shall be Including VAT.

Contact details
Please supply details of the certified and expert person(s) at your organisation who can be contacted and verified by AAUP. Please give their name, title, address and location, telephone number, fax number and e-mail address.

Company details
a) Please give details of your company, stating its full registered address and company registration number and all legal documents.
b) Please set our details of the partner and vendor company and specify the relationship between it and your company and provide detailed level of partnership and certification.
Your Organisation's staff
a) Please give details of your staff numbers, skills, duties and locations those who will be associated with the proposed work. Please set out any key skills or employee dependencies and the availability of replacement skills in those areas.
b) Please explain the organisational and management structure of your organisation (including an organogram of your executive management) and the roles and responsibilities of the management teams involved in relation to the services in the proposed solution.

Your history, approach, vision and values
a) Please describe in brief terms, your organisation's history and the history of provision of outsourcing services.
b) Over what period of time have you been providing services which are similar to those which are the subject of our request.
c) Please provide details of your corporate and business values and how this affects your organisation and the services it offers.

Customers
Please supply a list of customers to whom similar services to our request.

References
Please provide references of work done in the past and the success ratio where services were provided similar to our request.

Standards and procedures
a) Please provide details of your quality assurance processes and management systems and if applicable any quality related accreditations or certifications you hold.
b) Please set out your policies, procedures and processes in relation to the protection of all information and data in relation to the services and in relation to other security and confidentiality matters.
c) Please provide a brief risk management overview of the risks that you foresee in the delivery of each area of the requirements you are responding to. Please categorise these risks according to whether they are risks for AAUP, for you, or risks that are to be shared jointly. Please specifically state how you propose to manage and/or mitigate these risks.
d) Please confirm that all goods, services, software and intellectual property which would be provided or supplied by you in the course of the provision of the services are compliant with applicable regulatory framework.
e) Please give details of the systems and processes that are intended to be used to ensure security of personal customer data.

Support and Training

A. Support should be available 24/7/365 according to follow the sun principle
B. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response
C. Official training is a must for AAUP responsible team and security member.

Other capabilities
Please set out any additional capabilities or other services you provide beyond the scope of those contained in the proposed solution which may be of interest to AAUP.