التاريخ:2024/12/4
الرقم: ص2038/2024/2

رابطة الجامعيين / محافظة الخليل
جامعة بوليتكنك فلسطين
لجنة العطاءات المركزية
كراسة الشروط والمواصفات الفنية لعطاء

نظم الحماية لمركز البيانات في الجامعة

عطاء رقم: ص2038/2024/2

ثمن الكراسة بمبلغ(NIS200)

(مئتان شيكل فقط)

استلام كراسة الشروط ابتداء من يوم الاربعاء الموافق 2024/12/4

تسليم الكراسة يوم الاربعاء 2024/12/18

مع أطيب أمنيات

دائرة العطاءات والمشتريات المركزية

المحتويات :

.1	اسم العطاء	1
.2	الفهرس	2
.3	الإعلان	3
.4	ملاحظات عامة	4
.5	تعهد والالتزام	5
.6	تعليمات للمشاركين.	6
.7	عموميات وجدول المواصفات والكميات والأسعار	8
.8	معلومات عن الشركة	8

إعلان عن عطاء
نظم الحماية لمركز البيانات في الجامعة
الرقم: 2038/2024/2

تعلن رابطة الجامعين/ جامعة بوليتكنك فلسطين/ مركز الحاسوب عن طرح عطاء نظم الحماية لمركز البيانات في الجامعة ، وذلك ضمن الشروط والمواصفات الموضحة في كراسة وثائق العطاء، فعلى الشركات الراغبة بالدخول في العطاء إتباع الآتي: -

1. استلام الكراسة كاملةً من دائرة من العطاءات والمشتريات المركزية في مقر الجامعة/ ضاحية البلدية، **مقابل دفع مبلغ (200 NIS) مئتان شيكل غير مستردة تودع في حساب رابطة الجامعيين والجامعة رقم 30300 في البنك الإسلامي الفلسطيني اعتباراً من يوم الاربعاء الموافق 2024/12/4**
2. إرفاق شيك بنكي أو كفاله بنكية بقيمة 5% من قيمة العطاء وبظرف منفصل، على أن تكون الكفالة البنكية سارية المفعول لمدة لا تقل عن مئة وعشرين يوماً.
3. تسليم كراسة العطاء مع كافة التفاصيل بالظرف المختوم **حتى الساعة الثانية عشرة والنصف ظهرا من يوم الاربعاء الموافق 2024/12/18 لدائرة العطاءات والمشتريات المركزية – رابطة الجامعيين.**
4. الأسعار بالشيكل، شاملة ضريبة القيمة المضافة.
5. الرجاء إرفاق شهادة خصم مصدر سارية المفعول مع العطاء.
6. لجنة العطاءات غير ملزمة بقبول أقل الأسعار، وبدون إبداء الأسباب.

لمزيد من الاستفسار يمكن الاتصال مع الاستاذ وائل عواد 0569004173 خلال اوقات الدوام الرسمي

ملاحظة: - أجور الإعلان على من يرسو عليه العطاء

الادارة

الملاحظات العامة

عطاء نظم الحماية لمركز البيانات في الجامعة

الرقم: ص2/2024/2038

يرجى مراعاة الآتي :-

1. يجب أن يكون المتقدم للعطاء شركة متخصصة في المجال
2. الأسعار **بالشيكل**، شاملة ضريبة القيمة المضافة.
3. الرجاء إرفاق شهادة خصم مصدر سارية المفعول مع العطاء
4. لجنة العطاءات غير ملزمة بقبول أقل الأسعار، وبدون إبداء الأسباب.
5. يحق للجنة العطاءات تجزئة العطاء
6. بحق للجنة العطاءات زيادة أو إنقاص الكميات.
7. يكون السعر وفقاً للشروط الواردة في كراسة العطاء.
8. الإعلان بالجريدة وكراسة الشروط الفنية للعطاء والاتفاقية وحدة واحدة وتقرآن معاً.
9. أجور الإعلان على من يرسو عليه العطاء.

تعهد وإقرار

أنا الموقع اسمي أدناه / قرأت الشروط واطلعت على المواصفات والبنود والتزمت بها التزاماً كاملاً وألتزم بالأسعار المقدمة من قبلي ، وأتعهد بتقديم براءة ذمة "خصم مصدر" من ضريبة الدخل سارية المفعول ومرفقة بالفاتورة الرسمية كما تعتبر هذه الثبوتيات أساسا لدفع المستحقات اللازمة للمورد.

وبناءاً على ذلك تمت المصادقة والتوقيع.

السادة / الشركة:_____

رقم المشغل المرخص:_____

العنوان:_____

رقم الهاتف:_____

رقم الفاكس:_____

التوقيع والخاتم

تعليمات للمشاركين بالعطاء

حضرات السادة : شركة_____ المحترمين

عطاء نظم الحماية لمركز البيانات في الجامعة

الرقم: ص2038/2024/2

للمشاركة في العطاء ما يلي:-

1. تعتبر مقدمة كراسة الشروط والمواصفات وإعلان الجريدة جزءا لا يتجزأ وتقران معا.
2. يجب على صاحب العطاء التوقيع على وثائق العطاء كما يجب ختم العرض وكافة مرفقاته بخاتم صاحب العطاء.
3. لايعتمد أي تعديل في الكراسة بسبب ما يدونه المتقدم من اشتراطات، ما لم تقبل بها لجنة العطاءات المركزية.
4. يجب على الشركة أن يضع أسعاره رقماً وكتابة على النموذج ويرفض أي عرض يحدث فيه المتقدم تشويشاً في أسعاره ، واللجنة غير مسؤولة عن أية أخطاء قد يرتكبها المتقدم في وضع الأسعار.
5. على كل مناقص أن يرفق بالعطاء – لصالح رابطة الجامعين– تأمينا للدخول في العطاء كفالة بنكية أو شيك مصدق من قبل البنوك المحلية بقيمة 5% خمسة بالمائة من قيمة عرضه ولا ينظر في العروض الغير معززة بتلك التأمينات.
6. في حالة تأخير المورد عن الاعمال المحالة عليه تحسب غرامات التأخير بنسبة 1.5%، عن كل يوم تأخير، ومصادرة قيمة التأمين المرفق بالعطاء وقيده إيرادا للرابطة.
7. لاحقا لبند رقم (6) تقوم لجنة العطاءات المركزية بتنفيذ العطاء مباشرةً بالأسعار والشروط والطريقة المناسبة، من السوق المحلي مضافاً إليه (15%) من ذلك الفرق كنفقات إدارية.
8. عدم وجود أي تحفظات لها علاقة بسعر صرف العملات الأجنبية ويجب أن تكون الأسعار ثابتة حتى إتمام الالتزامات الفنية للمناقص في البند وصرف المستحقات وسيتم استبعاد أي عرض يوجد به تحفظات مرتبطة بأسعار صرف العملات الأجنبية.
9. يقدم العرض على النموذج أدناه ولا يحق إدخال أية تعديلات على وثائق العطاء. وإذا رغب الشركة تقديم ملاحظات أو عرض بديل عليه تقديم ذلك بمذكرة خاصة منفصلة شريطة تقديم العرض الأصلي كما هو، ولرابطة الجامعيين حق النظر بالمذكرة أو رفضها.
10. تكون المحاسبة وصرف جميع المستحقات للمناقص بعد الاستلام النهائي من لجنة الاستلام وعلى ضوء نتائج الفحص والاستلام حسب الأصول.

11. لا يجوز تحميل بند على بند آخر ولرابطة الجامعيين الخيار في إلغاء أي بند وتبقى أسعار البنود الأخرى ملزمة للشركة.
12. تعتبر الشروط العامة والفنية المطبقة في النظام العام للمشتريات جزاءا مكملا لهذه الشروط في عطاءات رابطة الجامعيين.
13. يجوز للمناقص سحب عرضه بمذكرة موقعة منه وتودع في صندوق العطاءات قبل الموعد المحدد لفتح العطاء.
14. لا يجوز لصاحب العطاء التعديل أو المحو أو الطمس في قائمة الأسعار وأي تصحيح يجريه صاحب العرض عليها يجب إعادة كتابته رقماً وكتابة والتوقيع عليه وختمه.
15. إذا بلغت فئات الأسعار التي جرى عليها التعديل أو المحو أو الطمس أكثر من 10% من قائمة الأسعار جاز للجنة العطاءات والمشتريات المركزية استبعاد العرض.
16. يعتبر العرض المقدم من الشركة ملزماً له.
17. **آخر موعد لتسليم العروض حتى الساعة الثانية عشرة والنصف ظهرا من يوم الاربعاء الموافق 2024/12/18.**

#	Item and Specifications	Amount in ILS
1	**Web Application Firewall (WAF) Solution** **1. Introduction** Palestine Polytechnic University invites qualified vendors to submit proposals for providing a Web Application Firewall (WAF) solution to protect our web applications and servers from malicious attacks, ensure compliance, and enhance our overall cybersecurity posture. The WAF solution will be deployed to secure web servers and must integrate seamlessly with our existing FortiGate 900G firewall and network infrastructure. **2. Project Objectives** a. Ensure robust protection against OWASP Top 10 vulnerabilities. b. Provide scalability to handle high traffic and user concurrency during peak times. c. Enhance visibility into threats with advanced logging and analytics. d. Offer seamless integration with existing systems for centralized management and monitoring. **3. Scope of Work** The scope of this RFP includes the following: 1. WAF Solution:	

a. Delivery, installation, and configuration of a WAF appliance or software.
b. Protection for web servers with scalability options.
c. Layer 7 protection for web applications, APIs, and mobile applications.
d. SSL/TLS inspection and offloading.

2. Integration:
   a. Integration with FortiGate 900G and other existing infrastructure.
   b. Compatibility with LDAP, RADIUS, and external authentication systems.
3. Technical Specifications:
   a. Machine Learning and Threat Analytics.
      - Detect and block threats with machine learning while minimizing false positives.
      - Threat analytics to identify attack patterns and separate real threats from informational alerts.
      - Advanced bot mitigation to protect web assets without impacting legitimate users.
   b. Web Application Security
      - Protection for APIs, including risks for mobile applications.
      - OWASP Top 10 protection.
      - Features such as automatic profiling (whitelisting), web server and application signatures (blacklisting), IP reputation, geolocation, and HTTP RFC compliance.
      - Support for HTTP/2 and HTTP/3.
      - Protection against attacks including:
        - SQL Injection
        - Cross-Site Scripting (XSS)
        - Cookie or form tampering
        - Session hijacking
        - Web defacement prevention
        - Forceful browsing
        - Buffer overflows
        - Brute force
        - Layer 4 and 7 Dos and DDos
        - SQL LDAP and XPath injections
        - Bad Robot
        - Generic attacks
        - Broken access control
   c. Performance and Scalability
      - Minimum L7 WAF throughput of 700 Mbps.
      - Support for HTTP/S protocols (0.9/1.0/1.1/2.0/3.0), WebSocket, and XML.

- Minimum Concurrent connections:
  - HTTP: 1.2 million
  - HTTPS:100,000
- Interface support: 4 x 1 Gigabit Ethernet copper, 4 x SFP GE, with fail-open (bypass) for two interfaces.

d. Management and Administration.
- Web-based user interface and command-line interface (CLI).
- Active/Active and Active/Passive High Availability (HA) clustering.
- REST API for management and integration.

e. Reporting and Logs
- Detailed logs for traffic, attacks, and system events.
- Reports on-demand and scheduled for auditing and analysis.

4. Management and Reporting:
   a. Centralized management interface with role-based access control.
   b. Advanced logging, monitoring, and customizable reporting.
   c. Integration with Security Information and Event Management (SIEM) tools.
5. Training and Support:
   a. Administrators training for WAF management.
   b. 3-year warranty and licensing, including
      - 24/7 technical support and maintenance
      - Advanced hardware replacement (next business day).
      - Firmware and general upgrades
      - Application Security, IP Reputation, Antivirus, Cloud Sandbox, Credential Stuffing Defense, Advanced Bot Protection, and Data Loss Prevention services.

4. Proposal Requirements

Vendors must include the following in their proposals:

1. Company Information:
   a. Company profile and relevant experience.
   b. References for similar projects in educational institutions or similar environments.
2. Technical Proposal:
   a. Detailed description of the proposed solution and its capabilities.
   b. Deployment options (on-premises, cloud, hybrid).
   c. Integration plan with existing infrastructure**.**
3. Performance Specifications:
   a. Throughput capacity (e.g., Mbps/Gbps).
   b. Maximum concurrent sessions supported.
   c. Scalability options**.**

4. Cost Breakdown:
   a. Licensing fees (perpetual or subscription-based).
   b. Deployment and integration costs.
   c. Support and maintenance costs (minimum of 3 years).
5. Implementation Plan:
   a. Estimated timeline for delivery and deployment.
   b. Milestones and deliverables.

5. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

a. Technical capabilities
b. Cost-effectiveness
c. Integration with existing infrastructure
d. Vendor experience and references
e. Training and support

2

Data Center Switch: preferred FortiSwitch 1024E

Specifications:

Total Network Interfaces (Proposed)	24x 10GE SFP+ ports and 2x 100GE QSFP28 ports
10/100/1000 Service Ports	1
RJ-45 Serial Console Port	1
Form Factor	1 RU Rack-Mount Appliance
Power over Ethernet (PoE) Ports	—
PoE Power Budget	—
Switch Capacity (Duplex)	880 Gbps
Packets Per Second	1039 Mpps
MAC Address Storage	64,000
Network Latency	< 1us
VLANs Supported	4k
IPv4/IPv6 Routing	Yes
Link Aggregation Group Size	up to 24
Total Link Aggregation Groups	Up to number of ports
Queues/Port	8
Packet Buffers	8 MB
Memory	8GB DDR4
Flash	32MB NOR
Drive	8GB SSD

3	**Endpoint Detection and Response (EDR) Specifications** 1. **Real-Time Threat Detection and Protection** a. Automated endpoint protection with AI/ML for real-time detection and prevention of zero-day malware, ransomware, phishing, and advanced threats. b. Inline blocking for zero-day malware and phishing sites. c. Comprehensive protection for pre-infection and post-infection scenarios. 2. **Incident Response and Remediation** a. Automated incident classification and response actions: isolate devices, terminate processes, remove malicious files, rollback system changes, and notify users. b. Full visibility of the attack chain with patented code tracing. c. Contextual incident response using classifications and endpoint group data. 3. **Advanced Security Features** a. Virtual patching to mitigate system and application vulnerabilities. b. USB device control and application control to lock sensitive systems like POS devices. c. Integration with third-party solutions like NGFW, NAC, SIEM, and sandbox environments. d. Offline protection for disconnected endpoints. 4. **Threat Intelligence** a. Real-time threat intelligence feeds via cloud services like FortiGuard. b. Static code analysis and deep learning-powered VM-less code emulation for enhanced threat detection. c. Network threat detection to identify botnet activities, malicious URLs, and network attacks. 5. **IoT and Rogue Device Security** a. Discovery and control of unprotected, unmanaged, or rogue IoT devices. b. Vulnerability assessments and proactive risk mitigation policies. 6. **Management and Reporting** a. Centralized management interface with role-based access control. b. Advanced logging, monitoring, and customizable reporting. c. Recommendations for response actions to optimize security resources. 7. **Deployment and Scalability** a. Deployment options: On-premises, cloud, or hybrid environments. b. Lightweight agents with minimal system performance impact. c. Supports up to date versions of Windows, macOS, Linux, and VDI environments (e.g., VMware, Citrix). 8. **Platform and Compatibility** a. Supported Platforms: a. Windows: XP SP2 to 11, and Server 2003 SP2 to 2022.	

	b. macOS: Versions 10.11 (El Capitan) to 14 (Sonoma). c. Linux: RHEL, CentOS, Ubuntu LTS, Oracle Linux, Amazon Linux, SUSE. d. VDI Environments: VMware Horizons, Citrix XenDesktop. b. Includes proactive risk mitigation for IoT and extended detection and response (XDR). 9. **Warranty and Support** o Minimum **3 years warranty** with 24/7 support, software updates, and access to cloud services.	
*	**Total in ILS**	

المجموع كتابة:_____

خاص بالشركة-:

اسم الشركة:_____

رقم المشغل المرخص:_____

العنوان:_____

رقم الهاتف:_____ رقم جوال:_____رقم الفاكس:_____

التوقيع والختم الرسمي