الشروط الخاصة

احمد حسن
محمد عمر
أمل أحمد

أولاً: نطاق المناقصة

يتضمن المناقصة مرحلتين أساسيتين:

١. انشاء منظومة داتا سنتر متكاملة بالموقع الاحتياطي تعتمد على بنية موحدة تشمل الخوادم وانظمة التخزين وشبكات الربط ومنصات الادارة الافتراضية مع ضمان التكامل مع مركز البيانات الرئيسي لتحقيق مستوى عالي من الجاهزية والمرونة التشغيلية ودعم خطط التعافي من الكوارث.

٢. تحديث تراخيص وحدات الحماية بالفروع وتطبيق انظمة الامن السيبراني الحديثة مثل SIEM – SOAR وتقنية الخداع الدفاعي وتنفيذ اختبارات اختراق معتمدة لقياس الوضع الأمني ومعالجة الثغرات.

ثانياً: أهداف المناقصة

١. إنشاء منظومة داتا سنتر متكاملة بالموقع الاحتياطي تشمل الخوادم، والتخزين، والشبكات، ومنصة الإدارة الافتراضية، مع ربطها بالمركز الرئيسي لتحقيق استمرارية الأعمال.

٢. تحقيق تكامل كامل بين المركز الرئيسي والاحتياطي عبر ربط أنظمة التشغيل، وقواعد البيانات، والتطبيقات الحيوية، لتفعيل خطط التعافي السريع.

٣. تطبيق منظومة أمن سيبراني موحدة تشمل SIEM، SOAR، Sandbox، Deception، ADC، MFA.

٤. تحديث تراخيص وحدات الحماية بالفروع لضمان التحكم المركزي وسياسات أمان موحدة.

٥. تحسين أداء التطبيقات الداخلية والخارجية باستخدام منصة تسريع تطبيقات الويب وتوزيع الأحمال.

٦. تنفيذ اختبارات اختراق معتمدة لمعالجة أي تهديدات محتملة قبل الاستهداف.

٧. تعزيز جاهزية الشركة الرقمية عبر بنية تحتية آمنة وقابلة للتوسع وتحقق التكامل بين موقعي التشغيل.

احمد حسـ
محمد عمر
امل احمد

ثالثاً: الشروط الخاصة

١. الأسعار شاملة جميع الضرائب، ويلتزم مقدم العطاء بمراجعة القطاع المالي بالشركة للوقوف على كافة الاستقطاعات والضرائب الخاصة بالعملية.

٢. يُشترط على المورد المتقدم تقديم عرض فني مفصل يتضمن الرد على جميع البنود الواردة بكراسة الشروط بندًا بندًا توضيحًا وتعليقًا، مع تقديم مواصفات فنية كاملة للمنتج أو الحل المقدم والكتالوجات الاصلية، ويُرفض أي عرض يكتفي بختم أو التوقيع على كراسة الشروط دون تقديم تفاصيل فنية مكتوبة ومعتمدة ويُعد عدم تقديم الرد التفصيلي سببًا كافيًا لاستبعاد العرض فنيًا.

٣. تلتزم الشركة المنفذة بتقديم:

- عرض تقديمي شامل للعملية.
- جدول زمني واضح للتنفيذ.
- سابقة أعمال تثبت تنفيذ مشروعات مماثلة لهيئات أو شركات أخرى.

٤. يشترط أن يكون المورد معتمدًا لدى الشركة المُصنّعة بمستوى شراكة لا يقل عن Select أو ما يعادله لدى الشركات الأخرى، مع تقديم شهادات اعتماد رسمية وسارية تُثبت مستوى الشراكة وقدرة المورد الفنية على تنفيذ الحلول محل الطرح ولا يُقبل مستوى Registered بأي حال باعتباره مستوى ابتدائيًا غير مؤهل لأعمال المؤسسات.

٥. فترة الضمان **5 :سنوات تبدأ من تاريخ التوريد والفحص.**

- الصيانة مجانية وشاملة قطع الغيار لجميع الأجهزة والبرمجيات ضد عيوب الصناعة.
- الشركة المنفذة مسئولة عن إصلاح أي خلل أو عيب يظهر خلال فترة الضمان على نفقتها الخاصة.
- الالتزام بتوفير الدعم الفني طوال فترة الضمان.

٦. بخصوص البند رقم (١) مع العرض الفني والمالي للبند المقدم يلتزم المورد خلال فترة الضمان والدعم الفني الممتدة لخمس سنوات للبند بتقديم دراسة فنية كاملة وعرض سعر تفصيلي (Technical & Financial Proposal) لتنفيذ أعمال إعادة تهيئة وإعادة هيكلة منصة الـ Virtualization الحالية بالشركة – أيًا كان موقع تشغيلها – بما يحقق التكامل التشغيلي الكامل وتوحيد بيئة العمل بين مراكز البيانات , ويعتبر السعر المقدم من المورد في هذا الخصوص سعرًا ملزمًا طوال فترة الضمان والدعم الفني، ولا يجوز تعديله أو المطالبة بتغييره أو إضافته خلال هذه المدة تحت أي ظرف، وذلك دون الإخلال بحق الشركة في تقرير تنفيذ أو عدم تنفيذ هذه الأعمال وفقاً لخططها وأولوياتها المستقبلية ودون أي التزام مالي عليها .

٧. البنود أرقام (٢ **الى** ٩) الخاصة بتحديث تراخيص أجهزة الحماية للفروع (FortiGate 61E)، ومنظومة Forti Sandbox، ومنظومة إدارة وتحليل الأحداث الأمنية (SIEM)، ومنظومة إدارة الاستجابة للحوادث الأمنية (SOAR)، ومنظومة توزيع الاحمال وتسريع تطبيقات الويب (ADC) وهكذا بنودًا مترابطة ومتكاملة وغير قابلة للتجزئة مع التزام المورد بتوفير مهندس متخصص (Resident Engineer) خلال السنة الأولى من مدة الضمان وتقديم السيرة الذاتية الخاصة به ، للعمل بنظام التواجد الدوري بالشركة وفق جدول يتم الاتفاق عليه مع الشركة، وذلك لمتابعة التشغيل الفعلي للمنظومات الأمنية (Firewall – Sandbox – SIEM – SOAR – ADC ... إلخ)، وتنفيذ أعمال المراقبة والتحسين المستمر، وسرعة معالجة أي أعطال أو إنذارات، وضمان استقرار وربط وتكامل مكونات البنية الأمنية بالشركة طوال فترة التشغيل.

٨. ويُشترط توريدها وتنفيذها كوحدة متكاملة من خلال نفس الجهة، نظرًا لضرورة تحقيق التكامل الفني والتشغيلي بينها وبين منظومة Fortinet Security Fabric القائمة بالشركة، وضمان توافق الإعدادات، والربط اللحظي بين مكونات الأمن المختلفة (Firewall – Sandbox – SIEM – SOAR- ADC…Etc.).

٩. لضمان تكامل المنظومة وسرعة الاستجابة للحوادث وتحقيق التشغيل المستقر لمنظومة أمن المعلومات، يشترط أن يكون نظام إدارة وتحليل الأحداث الأمنية (SIEM) البند رقم (٤) ونظام إدارة الاستجابة للأحداث الامنية (SOAR) البند رقم (٥) يعملا بشكل متكامل (Native Integration) في كلا الاتجاهين دون الحاجة إلى أدوات ربط خارجية أو طرف ثالث، وبما يضمن توافر Playbooks جاهزة، وتكامل مباشر مع مكوّنات البنية الأمنية الحالية بالشركة.

احمد
محمد عمر
أمل

رابعاً: مخرجات المشروع المتوقعة

- داتا سنتر متكاملة.
- شبكة آمنة ومحمية وفق أحدث المعايير العالمية.
- أنظمة عالية التوافرية تضمن استمرارية الخدمة.
- سياسات أمن موحدة ومتكاملة بجميع الفروع.

خامساً: التزامات مقدم العطاء والشركة المنفذة

١. المعاينة الميدانية

- يجب على مقدم العطاء معاينة أماكن تنفيذ العملية بجميع مواقع الشركة ومعاينة أجهزة الحاسبات الرئيسية والسويتشات الحالية.
- تعتبر هذه المعاينة "معاينة نافية للجهالة" حتى يتسنى للشركة المنفذة عمل الربط والتكامل الكامل بين الأجهزة الحالية والأجهزة الجديدة الموردة والمركبة والمشغلة.
- الغرض من ذلك تفادي أي سهو أو نسيان في تنفيذ المتطلبات الواردة بكراسة الشروط والمواصفات.

٢. إدارة المشروع والدعم الفني

- تلتزم الشركة الموردة بتوفير مدير مشروع بشكل دائم لمتابعة الأعمال وتسليمها بشكل كامل.

٣. التوريد والتركيب والتشغيل

- يلتزم مقدم العطاء بتوصيل جميع الأجهزة المطلوبة بالشبكة الداخلية والخوادم مع تأمينها بشكل كامل.
- جميع التركيبات لأي مكونات خاصة بالعملية تقع تحت مسئولية مقدم العطاء وتتم بواسطة متخصصين من جانبه.
- مسئولية تركيب وتشغيل الأجهزة والتجهيزات المطلوبة، بما في ذلك الإعدادات اللازمة، وتجهيزات مكان التركيب (كابلات – وصلات – تجهيزات كهربائية) تقع بالكامل على مقدم العطاء.
- يتعهد مقدم العطاء بضمان توافق الأجهزة الجديدة مع الأجهزة ونظم التشغيل والبرامج الحالية بالشركة، بما يشمل كروت الترقية أو تحديثات نظم التشغيل عند الحاجة.

٤. المواصفات الفنية للأجهزة الموردة

- جميع الأجهزة والمعدات الموردة يتم تسليمها شاملة:
  - أدلة التشغيل والاستخدام.
  - الوسائط الممغنطة أو المدمجة (نسخ أصلية).
- جميع الأجهزة الموردة يجب أن تكون متوافقة مع الظروف القياسية المصرية من حيث:
  - درجات الحرارة والرطوبة.
  - الجهد الكهربائي المستخدم (٢٢٠ فولت / ٥٠ هرتز).
  - توافق المقابس الكهربائية.
  - مقاومة الظروف البيئية الخاصة :مثل الأتربة، الاهتزازات، وانقطاع أو تذبذب التيار.

احمد
محمد عمر
أمل أحمد

٥. مدة التوريد

- يلتزم المتعاقد بتنفيذ أعمال التوريد والتركيب والتشغيل والتسليم والتدريب لكامل موضوع التعاقد خلال **6أشهر** من تاريخ استلام امر التوريد.

٦. العرض التقديمي الفني الإلزامي

- يلتزم المورد بتقديم عرض تقديمي عن تكامل المنظومة المقترحة مع المنظومات الحالية على **أسطوانة مدمجة (CD/DVD).** وفلاشه والعرض الفني المقدم بصيغة (pdf-word).
- يتم إخطار المورد بموعد العرض الفني، ويُحرر محضر لإثبات الحالة **إذا تم طلب تنفيذ العرض.**
- في حالة عدم تقديم العرض التقديمي يعتبر العرض **مرفوضاً فنياً.**
- يجب أن يتضمن العرض التقديمي البنود التالية:
  - كيفية ربط وتكامل جميع الأنظمة مع الفرع الرئيسي.
  - كيفية ربط وتكامل منظومة الأمن السيبراني وحماية البيانات مع الفرع الرئيسي.
  - كيفية ربط وتكامل منظومة السيرفرات مع الفرع الرئيسي.

٧. التزامات الشركة المنفذة

- تتحمل الشركة المنفذة **كافة نفقات النقل أو التركيب أو الاستبدال** لأي أجهزة موردة يتم نقلها من الفرع الاحتياطي إلى المقر الرئيسي أو العكس.
- تشمل مسئولية الشركة المنفذة:
  - النقل والتغليف الآمن للأجهزة.
  - التركيب والتشغيل والتكامل الكامل بين الأجهزة بالمقر الرئيسي والاحتياطي.
  - تنفيذ كافة أعمال الـ Installation أو الـ Configuration أو الـ Upgrade المطلوبة أثناء عملية النقل.

سابعاً: مكونات العرض الفني

١. المواصفات الفنية

- يجب كتابة المواصفات الفنية كاملة كما هي موضحة بجدول المواصفات لكل بند.
- إرفاق الكتالوجات الأصلية لجميع الأصناف المقدمة.
- في حالة تقديم صور من الكتالوجات يجب أن تكون معتمدة ومختومة من الشركة مقدمة العطاء.

٢. خدمات الدعم الفني والصيانة بعد الضمان

- تقديم عرض فني مفصل للدعم الفني والصيانة لما بعد فترة الضمان.
- في حالة طلب الشركة الاستمرار بالدعم، يلتزم المورد بتقديم الخدمة لمدة 3أشهر على الأقل بعد انتهاء فترة الضمان.

٣. خدمات ما بعد البيع

- شرح تفصيلي لخدمات ما بعد البيع يشمل:
  - أماكن مراكز الصيانة.
  - إجراءات الإصلاح.
  - كيفية استلام وتسليم الأجهزة المعيبة واستبدالها.
  - وجود تواصل مع المورد vendorوعمل تدريب على النظام الجديد.

احمد حسن
محمد عمر
أمل أحمد

٤. **سابقة الأعمال**

- تقديم سابقة أعمال موثقة (أوامر توريد أو محاضر تسليم) لا تقل عن 6سنوات للماركة المقدمة.
- في حال كانت المدة أقل أو أكثر، يخضع ذلك لأسس ومعايير التقييم الفني المحددة لاحقاً بكراسة الشروط.

ثامناً: العطاءات المستبعدة

١. يحق للشركة استبعاد أي عطاء لا يحقق المستوى الفني المطلوب أو لا يلتزم بالشروط العامة والخاصة.

٢. استبعاد أي عطاء إذا كان خطاب الضمان الابتدائي مقترناً بأي قيد أو شرط.

٣. استبعاد أي عطاء يتضمن شروطاً إضافية أو تحفظات تخالف ما ورد بكراسة الشروط.

احمد حسن
محمد عمر
أمل أحمد

البند رقم (١) مركز بيانات متكامل (Integrated Datacenter)

1. General Requirements

- Solution is total solution managed from one Windows
- All licenses in this project must be Lifetime license perpetual license
- The solution must be covered by 5-year support direct from vendor
- Solution in Turnkey solution from one vendor with vendor rack.
- Vendor must have Support service center in Egypt support Arabic language
- Solution must be based on building block Arch.
- Solution must not depend on SW lock to HW
- The supplier is obligated to supply all the necessary requirements (technical, operational, electrical, construction, and software) for the full operation of the system, even if some requirements are not explicitly stated in terms and conditions. The supplier remains responsible for providing them if they are necessary for integrated operation.

2. Technical Requirement for Datacenter

2.1 Table of Requirements

Items	Description	Qty
1	Virtualization Platform	1
2	Unified Management Platform	1
3	Servers	5
4	Enterprise All NVMe SAN Storage	1
5	TOR Switches	2
6	ISCSI Switch for system Cluster 2QQ	2
7	Microsoft Windows server 2022 Licenses	20
8	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications. Other official training (SAP HANA database Operating & Administration – SAP Business One System Administration & Support – SUSE Linux Enterprise Server Administration) for four engineers in certified training center from vendor with international exam and full Accommodation.	

أ/ محمد عمر
أ/ أمل أحمد

2.2 Item 1 Virtualization Platform: Qty 1

Requirements	Description
Vendor	Orchestration, Automation and Management Platform and virtualization platform must be a complete integrated solution from same vendor to ensure full integration and harmony
License	All necessary licenses are provided. License Must be perpetual, subscription model not allowed only SNS require renewal.
	Provides licenses for all the devices offered
Function	Provides VM creation, modification, and lifecycle management.
VM Deletion Protection & Recovery Mechanism	The platform must include a mechanism to recover deleted VMs without requiring a full backup restore, using features such as recycle bin, snapshot recovery, or protection domain–based restoration
High availability	Must allow you to configure whether to enable HA for VMs upon storage faults or not to handle storage faults to ensure high service availability.

Snapshots	Allows you to create consistency snapshots for VMs. When a fault occurs, services can be quickly restored to the state at point in time when the snapshot was created.
SDN	Must Support interconnection with network overlay SDN. At least one node can be deployed to manage network overlay SDN.
Network Security	Must allow you to configure virtual switches. You can configure security groups, DHCP isolation, and broadcast suppression to ensure VM network security.
Passthrough	Supports SR-IOV passthrough. The software emulation layer is bypassed in network transmission, and data is directly allocated to VMs, reducing the I/O overhead at the software emulation layer.
Virtual switches	Virtual switches use principal and subordinate VLANs (MUX VLAN) to implement communication or isolation between VM network devices in the same port group. This reduces VLAN ID consumption and simplifies network maintenance.
Maintenance service	Provides 5-year 7 x 24 Response direct from Vendor

2.3 Item 2 Unified Management Platform: Qty 1

Requirements	Description
Vendor	Orchestration, Automation and Management Platform and virtualization platform must be a complete integrated solution from same vendor to ensure full integration and harmony
Support	Must Provide Management, Automation and Orchestration for virtualization, BareMetal, Hardware (Include Servers, Storage, IP & FC Switches) including the full management capabilities for existing Hardware such as existing servers and storages
License	All necessary licenses are provided. License Must be perpetual, subscription model not allowed only SNS require renewal.
	Provides licenses for all the devices offered
Management and automation capabilities	Allows the platform or software to support unified management of storage devices, switches (FC and IP switches), servers, hyper-converged infrastructure, and virtual resources, including the query of the following: basic device information, configurations, historical performance, resource usage, and device alarms.
	Supports full-link I/O path diagnosis from the perspective of VMs: I/O path topology information of virtual disks, VMs, hosts, switches, and storage devices is displayed on one UI.
	Supports multi-dimensional associated object analysis from the application perspective for object instances, including VMs, hosts, LUN, and storage, to quickly demarcate and locate faults.
	Supports predictive O&M. Administrators can customize check conditions to check the configurations, capacity, performance, availability, light-load resources, and recyclable resources of storage, compute, and network resources. If a violation condition is matched, an event will be generated, helping administrators identify and prevent risks in advance.
	Allow users to configure a check policy for a specified VM. When the threshold defined in the policy is reached, the CPU or memory of the VM will be automatically expanded. During the process, the VM is running properly and does not need to be restarted.
	Allows you to modify the CPU, memory, and disk hardware parameters of VMs in batches, improving O&M efficiency.
	Supports large-screen display. More than three types of large-screen display and more than 20 types of chart controls are preset. Users can customize the content displayed on large screens.

ا محمد س
محمد عمر
أمل أحمد

	Supports report statistics. The system periodically and automatically generates reports, with preset reports for more than 30 typical service scenarios, such as capacity, resource performance, and alarms. Users can customize report statistics.
maintenance service	Provides 5-year 7 x 24 Response direct from Vendor

العقود و المشتريات
عملية رقم (٨٥)
جلسة ١٤/١/٢٠٢٦

2.4 Item 3 Rack Servers: Qty 5

Requirements	Description
Chassis	Rack Mount Server 8X 2.5inch Chassis,
Power Supply	Dual Redundant Power supply at least 2000 W
Processor	Dual Intel Xeon Gold 6530 2.1GHz, 32C/64T, 16GT/s, 160M Cache
Memory	8 X Memory Module, DDR5 RDIMM 64GB,5600MHz,2Rank(4G*4bit),1.1V, ECC
Hard Disk	2 X SSD, 3.84TB SSD SAS Disk Unit (2.5")
Raid controller	9560-8i RAID Controller, PCIE 4.0 X8 ,4GB cache, RAID 0,1,5,6,10,50,60, Support Super Cap and Sideband Management
Connectivity	2 X Dual port 25Gbps NIC card
Warranty	Provides 5-year 7 x 24 Response direct from Vendor

2.5 Item 4 Enterprise All NVMe SAN Storage: Qty 1

Requirements	Description
Architecture	Controllers work in active-active mode. Service loads are balanced among all controllers
	Controllers can be expanded for future business growth. Number of controllers supported up to 8.
	Non-disruptive upgrade is supported. Controllers do not need to be restarted during the upgrade.
Controller	Must have at least 2 controllers, support expend to 4 controllers without adding extra controller enclosure.
Cache	At least 128GB total cache capacity
Interface	Must include 8 x 25GbE ports with SFP+
Max number of disks	Supports at least 800 disk slots
Redundancy	Supports RAID 5, RAID 6 and another redundancy technology which is able to tolerate simultaneous failure of three disks
Data Reduction	Provides data deduplication and compression
Hard Disk	At least 20 x 7.68 TB NVMe SSD
Capacity	At least 100TB usable capacity at RAID 6
	Supports linear capacity expansion. The minimum expansion unit is a single disk, and no additional enclosure is required.
Features	Provides secure snapshots, which cannot be deleted or modified to stronger data protection
	Supports QoS to intelligently allocate and adjust resources in file systems or tenants
	Supports Quotas for any directory as soft and hard quota
	Supports the clone function, which provides an entity copy for a snapshot and a source LUN

احمد
محمد عمر
أمل

	Supports active-active DR between two sites without additional gateway
Management and maintenance	Supports hot swap of SSDs, power modules, and interfaces without service interruption.
	Monitors the lifespan and displays the wear level and estimated remaining service life of each SSD.
	Supports capacity prediction at least 180 days in advance.
	Provides graphical management software with comprehensive functions, including disk array and volume management software. Provides graphical management, configuration and monitoring software for storage devices.
Warranty	Provides 5-year 7 x 24 Response direct from Vendor

العقود والمشتريات
عملية رقم (٨٥)
جلسة: ٢٤/ ١ /٢٠٢٦

2.6 Item 5 TOR Switch: Qty 2

Item	Requirement
Forwarding performance	Switching capacity ≥ 4 Tbit/s.
	Packet forwarding rate ≥ 1200 Mpps
Hardware specifications	# Fixed interface switch with a height of 1 RU
	Number of power module slots ≥ 2, power modules in 1+1 backup mode
	Number of fan module slots ≥ 5.
	Front-to-back and back-to-front airflow
Interface configuration requirements	support 48*25GE SFP28 port + 8*100GE QFP28 port offered: 20 Port *25GE SFP28 port +10Port *10GE SFP+
Forwarding Table Capacity	Support MAC Address of larger than 500K
	Support FIB IPv4 of larger than 1M
	Support ACL of larger than 30K
Layer 2 Features	The switch supports access, trunk, and hybrid modes.
	Inter-chassis link bundling technologies, such as M-LAG, vPC are supported.
	M-LAG/vPC) supports consistency check, lossless upgrade in maintenance mode, and protocol authentication.
	Dynamic MAC address entries, static MAC address entries, and blackhole MAC address entries
Layer 3 Functions	IPv4 dynamic routing protocols such as RIP, OSPF, IS-IS, and BGP
	IPv6 dynamic routing protocols such as RIPng, OSPFv3, IS-ISv6, and BGP4+
	BFD for OSPF, BGP, IS-IS, and static routes
	IPv6 ND and PMTU discovery
QoS احمد حسن محمد عمر امل احمد	Queue scheduling modes such as PQ, DRR, and PQ+DRR
	Congestion avoidance mechanisms such as WRED and tail drop
	Outbound ACLs, outbound ACL-based rate limiting, and outbound IPv6 packet statistics are supported.
	MAC address limiting based on VLANs, sub-interfaces, BDs, and VXLAN tunnels are supported.
	Interface error-down triggered by MAC address flapping is supported.
	Port/VLAN/BD-based broadcast/multicast/unknown unicast suppression is supported.
	VXLAN broadcast flood suppression is supported.
	Traffic shaping
Reliability	Bidirectional Forwarding Detection (BFD) 3.3 ms detection interval

	Data Plane Fast Recovery (DPFR) is supported.
	Data Plane Crossing Faults (DPCF) is supported
	VRRP, VRRP load sharing, and BFD for VRRP
	M-LAG access site fast switchover within 50ms (active-active access)
DC features	VXLAN, EVPN VXLAN, and communication between VXLAN and VLAN networks
	VXLAN over IPv6 and IPv6 VXLAN over IPv4 are supported.
	Weak security protocol/algorithm query and security enhancement are supported.
	Defense against DoS attacks, ARP attacks, and ICMP attacks
	Bindings of IP addresses, MAC addresses, interface numbers, and VLAN IDs
	Port isolation
	AAA, RADIUS, and TACACS authentication
Multicast	Multicast traffic suppression
	IGMP snooping
	IGMP snooping proxy
	Protocols such as IGMP, PIM-SM, and MSDP
Hyper-Converged Ethernet Features	PFC and PFC deadlock prevention are supported.
	RDMA, RoCEv2, and DCB are supported.
	AI ECN is supported.
	ECN overlay is supported.
	NSLB is supported.
Configuration and maintenance	Telemetry
	The reporting of ARP/FIB/ND changes through telemetry is supported.
	ERSPAN enhancement is supported.
	ERSPAN mirrored packet and ECMP load balancing are supported.
	IFIT is supported.
	Visualization of packet event packet loss and ultra-long latency.
	VXLAN OAM (VXLAN ping and VXLAN tracert) is supported.
	SNMPv1/v2/v3, Telnet, RMON, and SSH
	Configuration rollback is supported.
	Network-wide path detection is supported.
	Cached microburst status statistics is supported.
	PTP clock synchronization is supported.
	Boot Read-Only Memory (Boot ROM) upgrade and remote online upgrade
	ZTP technology that allows the configuration to be automatically delivered
Network traffic analyzer	Net Stream or Equivalent.
Warranty	Provides 5-year 7 x 24 Response direct from Vendor

احمد
محمد عمر
أمل أحمد

2.7 Item 6 ISCSI Switch for Cluster: Qty 2

Item	Requirement
Forwarding performance	Switching capacity ≥ 4 Tbit/s.
	Packet forwarding rate ≥ 1200 Mpps
Hardware specifications	# Fixed interface switch with a height of 1 RU

	Number of power module slots ≥ 2, power modules in 1+1 backup mode
	Number of fan module slots ≥ 5.
	Front-to-back and back-to-front airflow
Interface configuration requirements	support 48*25GE SFP28 port + 8*100GE QFP28 port offered: 20 Port *25GE
Forwarding Table Capacity	Support MAC Address of larger than 500K
	Support FIB IPv4 of larger than 1M
	Support ACL of larger than 30K
Layer 2 Features	The switch supports access, trunk, and hybrid modes.
	Inter-chassis link bundling technologies, such as M-LAG, vPC are supported.
	M-LAG/vPC) supports consistency check, lossless upgrade in maintenance mode, and protocol authentication.
	Dynamic MAC address entries, static MAC address entries, and blackhole MAC address entries
Layer 3 Functions	IPv4 dynamic routing protocols such as RIP, OSPF, IS-IS, and BGP
	IPv6 dynamic routing protocols such as RIPng, OSPFv3, IS-ISv6, and BGP4+
	BFD for OSPF, BGP, IS-IS, and static routes
	IPv6 ND and PMTU discovery
QoS	Queue scheduling modes such as PQ, DRR, and PQ+DRR
	Congestion avoidance mechanisms such as WRED and tail drop
	Outbound ACLs, outbound ACL-based rate limiting, and outbound IPv6 packet statistics are supported.
	MAC address limiting based on VLANs, sub-interfaces, BDs, and VXLAN tunnels are supported.
	Interface error-down triggered by MAC address flapping is supported.
	Port/VLAN/BD-based broadcast/multicast/unknown unicast suppression is supported.
	VXLAN broadcast flood suppression is supported.
	Traffic shaping
Reliability	Bidirectional Forwarding Detection (BFD) 3.3 ms detection interval
	Data Plane Fast Recovery (DPFR) is supported.
	Data Plane Crossing Faults (DPCF) is supported
	VRRP, VRRP load sharing, and BFD for VRRP
	M-LAG access site fast switchover within 50ms (active-active access)
DC features	VXLAN, EVPN VXLAN, and communication between VXLAN and VLAN networks
	VXLAN over IPv6 and IPv6 VXLAN over IPv4 are supported.
[illegible] محمد عمر أحمد أحمد	Weak security protocol/algorithm query and security enhancement are supported.
	Defense against DoS attacks, ARP attacks, and ICMP attacks
	Bindings of IP addresses, MAC addresses, interface numbers, and VLAN IDs
	Port isolation
	AAA, RADIUS, and TACACS authentication
Multicast	Multicast traffic suppression
	IGMP snooping

	IGMP snooping proxy
	Protocols such as IGMP, PIM-SM, and MSDP
Hyper-Converged Ethernet Features	PFC and PFC deadlock prevention are supported.
	RDMA, RoCEv2, and DCB are supported.
	AI ECN is supported.
	ECN overlay is supported.
	NSLB is supported.
Configuration and maintenance	Telemetry
	The reporting of ARP/FIB/ND changes through telemetry is supported.
	ERSPAN enhancement is supported.
	ERSPAN mirrored packet and ECMP load balancing are supported.
	IFIT is supported.
	Visualization of packet event packet loss and ultra-long latency.
	VXLAN OAM (VXLAN ping and VXLAN tracert) is supported.
	SNMPv1/v2/v3, Telnet, RMON, and SSH
	Configuration rollback is supported.
	Network-wide path detection is supported.
	Cached microburst status statistics is supported.
	PTP clock synchronization is supported.
	Boot Read-Only Memory (Boot ROM) upgrade and remote online upgrade
	ZTP technology that allows the configuration to be automatically delivered
Network traffic analyzer	Net Stream or Equivalent.
Warranty	Provides 5-year 7 x 24 Response direct from Vendor

احمد مسلم
محمد عمر
أمل أحمد

البند رقم (٢) تحديث تراخيص انظمة الجدار الناري بالفروع

Items	Description
1	This item includes the renewal and upgrade of licenses for nine (9) FortiGate 61E firewall appliances (FGT61ETK18022998-FGT61ETK18023199-FGT61ETK18023322-FGT61ETK18023572-FGT61ETK18023763-FGT61ETK18023771-FGT61ETK18023807-FGT61ETK18024283-FGT61ETK18024557) for a period of five (5) years, in addition to extending the license of the FortiGate 201F(FG201FT922926032) appliance to match the same five-year duration. This ensures unified license validity across all firewall devices, consistent security updates, and continuous technical support throughout the contract period.
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

البند رقم (٣) منظومة الساند بوكس

Items	Description
1	- Supply, install, and configure (1 Appliance) units of Fortinet Forti Sandbox for advanced threat detection and zero-day attack prevention. - The new appliances can cluster with the existing Forti Sandbox 500F currently deployed in the main datacenter to ensure seamless expandability or having sandbox running on both sites (Main and DR). - The unit must support seamless integration with FortiGate Firewalls, Forti Analyzer, and Forti Manager, providing automated malware analysis, real-time detection, and quarantine actions. - Licenses must include Full ATP, Dynamic Threat Intelligence, and Cloud Sandbox services for a period of five (5) years, with 24x7 support and firmware updates directly from Fortinet. - Contains at least 2 VMs for sandboxing and can be extended to 14 VM - Must Support Custom VM. - Must support Microsoft Windows Server 2019 and Linux. - Can contain up to 4 X 1GE RJ45 interfaces - Must not be deployed in line of the web-traffic or email traffic - Must be single centralized inspection sandbox box for web, email and file sharing storage with the ability to integrate with multiple security solutions in all network boarders. - Can integrate with WAF of same brand to inspect file uploading to web application - Can feed integrating devices and endpoints with signatures of malicious files to avoid spread of malicious files inside the network - The item also includes renewing and extending the license of the existing Forti Sandbox 500F for a full five-year period to ensure unified protection levels, synchronized validity, and seamless integration with the newly supplied sandbox appliances
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

البند رقم (٤) منظومة إدارة وتحليل الاحداث الامنية (SIEM)

Items	Description
1 احمد حسن محمد عمر أمل أحمد	- This item covers the supply, deployment, and operation of an integrated Security Information and Event Management (SIEM) system for centralized log collection, analysis, and real-time security event monitoring across all IT systems within the company. - The SIEM must include a built-in correlation engine capable of cross-domain event correlation (network, endpoint, identity, application, and infrastructure). - The solution is a core component of the existing Fortinet Security Fabric, currently deployed (FortiGate, Palo Alto, Forti Sandbox, Forti Web, ClearPass, EDR Trillix ...), and aims to: o Aggregate and analyze security logs from all network and infrastructure components. o Detect abnormal activities and potential cyber threats proactively. o Generate intelligent alerts and compliance reports. o Provide full integration with the upcoming Security Orchestration, Automation, and Response (SOAR) platform to enable automated incident handling. o Empower the company's Security Operations Center (SOC) with unified, real-time visibility. - The solution shall be delivered as a turnkey project, including installation, configuration, training, and five (5) years of licensing and 24×7 vendor support. - Solution must be Appliance based. - Solution must support 2500 EPS.

	- Solution must support at least 100 devices. - License must be perpetual, not time-bound, and shall not require renewal for continued operation. Expiry of support or maintenance shall not result in service interruption, feature limitation, or system shutdown During spikes license should have a reservoir to cover up license over usage without interrupting log collection or SIEM capabilities limitations . - Solution Must Support File Integrity Monitoring (FIM) for up to 50 devices and agentless UEBA - Solution must be easily scalable to increase more performance via adding more workers with no extra Lic/cost - Solution must automatically build a separate database with devices/assets in the network and automatically draw a network diagram for it - Solution must discover accurately infrastructure and security appliances components such as HW and SW modules and save that in the database - The SIEM solution should be able to comprehend, parse and normalize OT specific logs for further correlation and extended detection across OT environment - The SIEM solution should have Machine Learning Workbench to interact with different embedded Machine Learning Models to feed them with environment data to alert on anomalies while re-learning periods
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

البند رقم (٥) منظومة إدارة الاستجابة للحوادث الامنية (SOAR)

Items	Description
1 احمد محمد عمر	- This item covers the supply and deployment of a Security Orchestration, Automation, and Response (SOAR) system to complement the existing SIEM platform. - The system automates the analysis, correlation, and response to security incidents by executing predefined workflows (Playbooks) that reduce response time and human intervention. - The SOAR platform must support bi-directional integration with the SIEM, allowing automated response actions based on correlated events and feeding response results back into the SIEM. - The proposed SOAR platform shall: o Automate alert triage, incident investigation, and response actions. o Provide interactive playbooks for threat containment and remediation. o Offer centralized dashboards and KPIs for incident monitoring and performance tracking. o Support full case management and audit trail capabilities. o The solution shall be delivered as a turnkey project, including installation, configuration, training, and five (5) years of licensing and 24×7 vendor support. - Licensing Should allow predictable cost based on number of concurrent users only with unlimited number of user creation - SOAR License must be perpetual, non-expiring, and not subscription-based, Expiration of support or maintenance shall not impact system operation, playbooks execution, or automation capabilities and 2 User Logins (not named) Included. - The solution should support on-prem deployment and Solution must be VM based. - The system should have an in-life connector update mechanism that allows vendor connector updates between software releases. - The system should have a selection of vendor supplied and validated connectors for integration with 3rd party systems - Connector documentation must be available - Solution must have at least 300+ integration connectors - Solution must have at least 2600 playbooks including cases, samples and connector-related ones. - Admin must have the ability to export Playbook including all its saved versions (similar to SVN/GIT) - Solution must support restarting the playbook from the previously failed playbook step - Solution must allow the user to run the playbook from within the playbook editor. - Solution must support creating playbooks with a visual interface - The SOAR solution should have an embedded Recommendation Engine with multiple built in Machine Learning Models to baseline ingested alerts and provide related alerts and recommended playbooks to run accordingly. - The SOAR solution be able to investigate on OT assets discovered over the SIEM solution. - The SOAR solution must provide an embedded and automated case management module covering the full incident lifecycle, including alert-to-incident conversion, analyst assignment based on configurable conditions, shift-aware handling, and seamless handover between analysts to ensure uninterrupted SOC operations.

	- The playbook builder should support: o Manual actions and tasks - Decision making and approval steps o Nested playbooks - Logical conditions and loops - Python execution for custom scripts o Rich text Emails - Visual playbook troubleshooting o Configurable ability to halt or continue on playbook step error o The ability to mark playbooks as active
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

البند رقم (٦) منظومة توزيع الاحمال وتسريع تطبيقات الويب (ADC)

Items	Description
1	- The proposed system (2 appliances) aims to enhance the performance and reliability of the company's web applications by intelligently distributing network traffic across multiple servers while ensuring continuous service availability. - The solution forms an integral part of the company's Web Security Layer, working in conjunction with Forti Web to provide comprehensive protection and high performance for all internal and external web applications. - The solution shall be delivered as a turnkey project, including installation, configuration, training, and five (5) years of licensing and 24×7 vendor support. **Performance:** - 20Gbps L4/L7 throughput at least - 200k L7 CPS at least - 20k SSL connection/sec with 2048 key size - 14Gbps compression throughput - 30 virtual administrative domains with no extra LIC - 4 X10Gbps interfaces sfp+ - 4 X1 Gbps copper 10/100/1000 interfaces - 4 X1 Gbps sfp based interfaces - 120 GB SSD storage inside for better performance **Features**: - Hardware based SSL-offloading and SSL-inspection - HTTP compression - The solution must have Global Server Load Balancing (GSLB) capabilities to distribute traffic intelligently across multiple data centers or sites based on availability, performance, and health status, without reliance on third-party external DNS services. - Link load balancer with no extra cost - Solution must have Web Application Firewall and Web Vulnerability Scanner - API Security (Open API, API-GW, API Discovery) - WAF (AL) Adaptive Learning Support - Credential Stuffing Defense - OWASP top 10 Compliance - Advanced Bot Protection - IP repetition feeds updates, preferred from same vendor, not third party - HTTP cashing - Support Scripting to extend built-in features - Support policy-based routing - Support policy based stateful firewall policies with no extra cost - SSL forward proxy for Secure traffic inspection - TCP offloading - Client connection persistence - TCP buffering - http rate limiting - L4 rate limiting - BW allocation using QOS - Authentication offloading locally or through LDAP or RADIUS - IPv6 support with IPv6 routing and IPv6 firewall rules - Support BGP and OSPF - Support VLAN tagging and port trunking - Support GEO-IP security and logs
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

المهندس
محمد عمر
[illegible]

العقود و المشتريات
عملية رقم (٨٥)
جلسة : ٢١ / ١ / ٢٠٢٦

البند رقم (٧) منظومة تقنية الخداع الدفاعي (Deception)

Items	Description
1	- Appliance should have 4 x GE Rj45 and 4 x GE (SFP) - Appliance should support up to 128 Vlans and 20 Deception VMs - License for 10 Vlans should be available from day 1 - The solution shall be delivered as a turnkey project, including installation, configuration, training, and five (5) years of licensing and 24×7 vendor support. - The deception-based threat detection solution must integrate with the SIEM to provide correlated, high-confidence security events and forensic context, enabling the SOAR platform to execute automated and orchestrated incident response workflows. Support Deception Type - Network IT Decoys emulation of full OS Decoys - Supports framework for customization of Decoys with a framework - Decoys have ability to joins Active Directory - Decoy types of support, emulation of common network devices, including TCP port emulation - Decoy support for vertical specialization, such as ICS - End Point Lures – create lures based on windows credentials, SSH/RDP profiles and mapping to network file shares Deployment Management Capabilities - Supports VLAN trunking to expose Decoys to multiple VLANs from central location - Supports extension of Decoy from central location (e.g. Datacenter) to remote branches, over L3 or L2 connection - Supports auto VLAN detection and addition to deployment networks - Support Wizard based approach to deployment Threat Detection and Response - Decoy Data Gathering – Solution MUST perform extensive data gathering from decoy, including source IP and credential used for connection, process started on Decoy, and full CLI history on decoy - Decoy reset – solution MUST have ability for users to specific decoy reset interval, to default to the state before any hacking attempts - Decoy Artifacts – solution MUST have ability to download artifacts such as PCAPs or executables dropped into Decoys for further analysis - Decoy content randomization – Solution MUST have ability to randomized decoy content (e.g. file names/types on SMB/SAMBA services - Decoy MUST support detection of Intrusions TO and FROM decoys, and IPS signatures are updated regularly. - Decoy MUST support Detect Malware dropped onto Decoy and ability to alert - Decoy MUST support categorizing any websites visited from Decoys Security Integrations - Solution MUST have ability to integrate into SIEM technology from same vendor - Solution MUST have ability to integrate with NGFW from same vendor for quarantine/banned IP, and ability to quarantine depending on severity of event.
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

احمد م
محمد عمر

البند رقم (٨) منظومة المصادقة المتعددة (Multifactor Authentication)

Items	Description
1	- The solution shall be delivered as a turnkey project, including installation, configuration, training, and five (5) years of licensing and 24×7 vendor support. - Performance: - Solution should be software based - Supports at least 500 users - Supports at least Total of 500 OTP tokens, whether SW or HW - Support Active-Passive HA and Config Sync HA Features: - Gives the ability to Authenticate end users via multiple Radius clients/supplicants - Can work as an LDAP server - Can integrate with back-end Radius server, LDAP server or windows Domain controller/Active directory - Can provide 2 factor Auth via providing OTP tokens (SW or HW) and/or certificate HW tokens - Can work as Certificate manager and distribute user certificates. - Can authenticate users via HW certificate tokens - Support user self-registration and password recovery - Support 802.1x Authentication - Support identity and role-based security policies in secured enterprise network without the need for additional authentication through integration with Active Directory - Can provide built-in Authentication portal for SSO - Support SAML SP/IdP Web SSO - Support Certificate management for enterprise VPN deployment - Support Secure Multi-factor/OTP Authentication with full support for HW / SW Token - The multi-factor authentication (MFA) solution must integrate with the SIEM platform to forward authentication logs, anomalies, and risk events for correlation, thereby enabling the SOAR platform to initiate automated response actions when suspicious access behavior is detected. Supports the following methods at least for SSO: - Mobility agent - Kerberos - Active directory polling - Login-portals - API - Radius accounting - Syslog
2	The supplier shall provide a comprehensive training program that includes on-site technical training at the customer premises, along with official vendor-accredited administration courses for three engineers, to be delivered in a certified training center fully approved by the vendor, including international exam vouchers and full accommodation, with all certificates issued as official globally recognized certifications

احمد حسن
محمد عمر
أمل أحمد

البند رقم (٩) خدمات اختبارات الاختراق الامنية Penetration Testing

Items	Description
1	**Objective:** - To perform a professional, standards-based penetration testing engagement to identify security vulnerabilities in the company's networks, systems, and web applications, evaluate risk levels, and provide detailed remediation guidance. **Scope:** - Internal & External Infrastructure, Pentest Estimated Man days (12) - Vulnerability Assessment (VA), Pentest Estimated man Days (25). - Web Application Test, Pentest Estimated man Days (40). - Wireless Penetration Test, Pentest Estimated man Days (1). - One retest after remediation to validate closure of high/critical findings. - Internal Infrastructure Penetration Testing, Wireless Testing, and Vulnerability Assessment must be performed on-site at BNSCWW premises. - Remote execution for any of these components is strictly prohibited unless prior written approval is granted by the Company. - External Testing and Web Application Testing may be performed remotely subject to coordination and approval. - The penetration testing activities shall be performed using industry-standard tools such as Nessus, Qualys, Nmap, Metasploit Framework, Burp Suite Professional, OWASP ZAP, Aircrack-ng, Kismet, or equivalent professional-grade toolsets. **Methodology:** - Based on recognized standards: OWASP, NIST SP 800-115, and PTES. - Combination of automated scanning and manual exploitation validation. - Testing types: Black-box and/or Grey-box, as defined by project scope. - No DoS or social engineering activities unless explicitly approved in writing. **Deliverables:** - Executive Summary Report – non-technical overview of risks and business impact. - Detailed Technical Report – vulnerabilities, CVSS v3.1 severity, PoC evidence, remediation plan. - Vulnerability Register – Excel/CSV format for tracking and follow-up. - Retest Report – verification of fixed issues. **Support & Duration**: - Testing window: as agreed, outside business hours where applicable. - Report delivery: within 14 working days after completion. - Includes one retest session free of charge. **Compliance and Certification Requirements** - The penetration testing shall be performed exclusively by a certified and accredited third-party security company specializing in vulnerability assessment and penetration testing. - The testing company must be independent (not the system supplier or system integrator). - The vendor shall submit, along with their proposal or clarifications, a valid Accreditation Certificate or ISO/CREST/ISec/OSCP organizational certification proving their authorization to conduct penetration testing. - The provided certificate (for example, ISEC accreditation) must be attached within the technical clarification documents and remain valid throughout the testing period. - The final penetration test report must be officially signed and stamped by the accredited third-party company.
2	**The training program (onsite) shall include:** - Full explanation of all findings and exploitation techniques. - Training on penetration testing tools used during the engagement. - Vulnerability management and hardening best practices. - Incident response fundamentals and log analysis. - Web application security basics (OWASP Top 10) And official Training Courses (CEH-CPENT-ECIH) for 3 engineers in certified training center from vendor with international exam and full Accommodation.

العقود و المشتريات
عملية رقم (٨٥)
جلسة ٢٤/ ١ /٢٠٢٦

احمد حسه
محمد عمر

البند رقم (١٠) تاور وركستيشن Tower Workstation

Feature	Description
Supported Software For all quantity (14 PC)	5 Windows 11 Pro for Workstations licenses, English, Arabic and 9 windows 22 server standard licenses
Processor	Intel® Xeon® w5-3435X (16 cores, up to 4.7 GHz Turbo, 270 W)
CHIPSET	Intel W790
RAM	128 GB: 4 x 32 GB, DDR5, 4800 MT/s, RDIMM, ECC
Memory slots	2 TB, 8 x 256GB, DDR5, 4800MHz, ECC
Hard Disk	512 GB Performance SSD, SED Ready - 2 TB, 7200 RPM, 3.5-inch, SATA, HDD, AG-Enterprise Class
Optical Drive	DVD+/-RW
Expansion slots	2 full-height Gen5 PCIe x16 slots
External I/O Ports	Front: (2) USB 3.2 Gen 1 ports USB 3.2 Gen 2 Type-C port with Power Share USB 3.2 Gen 2 Type-C port Universal audio port SD-card slot Rear: (3) USB 3.2 Gen 2 Type-C ports (2) USB 3.2 Gen 1 ports USB 3.2 Gen 1 port with Smart Power On RJ45 Ethernet port, 1GBE RJ45 Ethernet port, 10GBE Line-out port Serial port (2) PS2 ports
Graphics	Nvidia RTX A1000, 8GB GDDR6, 4 mDP
Audio	Realtek ALC3246-CGT Internal Speakers
Network Adapter	RJ45 Ethernet port, 1GBE RJ45 Ethernet port, 10GBE
keyboard	Vendor Wired Keyboard - KB216 - Arabic (QWERTY) – Black
Mouse	Vendor Wired Mouse - MS116 - Black
Support	ProSupport Next Business Day Onsite Service after remote diagnosis with HW-SW Support, 60 Month(s)
Screen	Vendor Screen 24 inch with USB ports
SMART UPS-2000VA	Battery Cell Composition Lead Acid, Black, Metal

احمد م
محمد عمر
أمل

جدول الكميات

امل احمد
احمد حسن
محمد عمر

جدول الكميات

م	اسم الصنف	العدد المطلوب
1	منظومة داتا سنتر متكاملة	1
2	تحديث تراخيص انظمة الجدار الناري بالفروع نسخ الكترونية	9
3	منظومة الساندبوكس	1
4	منظومة إدارة وتحليل الاحداث الامنية	1
5	منظومة إدارة الاستجابة للحوادث الامنية نسخ الكترونية	1
6	منظومة توزيع الاحمال وتسريع تطبيقات الويب	2
7	منظومة تقنية الخداع الدفاعي	1
8	منظومة المصادقة المتعددة نسخ الكترونية	1
9	خدمات اختبارات الاختراق الامنية	1
10	تاور وركستيشن	14

نظر

م/ دينا عمر سليمان

٢٢/١١/٢٠٢٥

العقود والمشتريات
عملية رقم (٨٥)
جلسة ١١/١/٢٠٢٦

م/ اماني مرسي

امل احمد
احمد
محمد عمر

اسس التقييم الفني للعطاءات

العقود و المشتريات
عملية رقم (٨٥)
جلسة ١٤ / ١ / ٢٠٢٦

يتم استبعاد أي عطاء لا يحصل على 80 %

خبره الشركة الموردة لا تقل عن ٦ سنوات في اعمال توريد الماركات العالمية المثيلة والمقدمة بالعرض الفني	٤٠ نقطه لعدد سنوات خبره ٦ سنوات وان قلت يتم التقييم بالنقاط لعدد سنوات الخبرة	٤٠
مدي تطابق المواصفات الفنية المقدمة من الشركة صاحبة العطاء مع المواصفات بكراسة الشروط الفنية	الالتزام بالمواصفات الفنية المطلوبة بكراسة الشروط	٥٠
مدي تكامل العرض الفني	وهو ان تستوفي الشركة بالعرض الفني المقدم منها يوم فتح المظاريف كافة مكونات العرض الفني والمطلوبة بكراسة الشروط دون الحاجه الي طلب استيفاء او توضيح من الشركة صاحبة العطاء وفي حالة طلب استيفاءات يتم خصم نقاط بناء علي ذلك	١٠

اسس التقييم المالي:

١. سوف يتم فحص العروض المالية المقدمة من الموردين وفقا للشروط المناقصة المذكورة من قبل بغرض التأكد من عدم وجود اخطاء حسابية في الجمع وغيره.

٢. **سيتم التقييم المالي للعطاءات المقبولة فنيا فقط**– سوف يتم التقييم لكل بند على حدي وسوف يتم اعطاء اقل العروض ماليا 100 درجة ويتم تقييم باقي العروض المالية نسبة الى اقل العروض ماليا كما يلي:

درجة التقييم المالي للعرض (او للبند) س = سعر اقل العروض (البند) X100 / سعر العرض (البند) المالي (س) المطلوب تقييمه

يتم استبعاد العروض في حالة حصول العرض (البند) على اقل من 80 %

التقييم النهائي للعطاءات:

سوف يتم التقييم النهائي للعطاءات بنظام الوزن النسبي وسوف يؤخذ تقييم العطاء الفني 80% والعرض المالي20% ليصبح إجمالي

درجات التقييم الكلية للعرضين المالي والفني ١٠٠ درجة وسوف يكون التقييم كالتالي:

درجة التقييم الكلية للعطا (س)=80 % X درجة التقييم الفني للعطاء(س) +20% Xدرجة التقييم المالي للعطاء(س)

وسوف يتم اختيار العطاءات ذو درجات التقييم الكلية الاكبر ليصبح هو العطاء الافضل ويتم اسناد العقد الية.

اللجنة

احمد حسن
محمد عمر

رئيس اللجنة

د/ [illegible]

لجنة

د/ [illegible]
٢٠٢٥/١١/٢٢