جامعة العلوم الإسلامية العالمية
عطاء رقم (2022/7)

موضوع العطاء :-
" نظام حماية الأجهزة الطرفية "

أخر موعد لبيع النسخ وتقديم الاستفسارات الساعة (1) الواحدة من بعد ظهر يوم الثلاثاء الموافق 28 /2022/6)

أخر موعد لتقديم العروض الساعة (2) الثانية من بعد ظهر يوم الثلاثاء الموافق (2022/7/5)

وسيتم فتح العروض بحضور مندوبي المناقصين الراغبين بذلك بطلب مسبق وبموجب كتاب تفويض خطي من الشركة أو المؤسسة في تمام الساعة (12)الثانية عشرة ظهراً يوم الاربعاءالموافق (7/6 /2022)

ثمن النسخة (25) خمسة وعشرون دينارًا غير مستردة .

يلتزم المناقص بإرفاق كفالة دخول العطاء (كفالة بنكية أو شيك مصدق أو مبلغ نقدي) بقيمة (3%) من القيمة الإجمالية ويستبعد كل عرض مخالف للشروط

أجور الإعلان على من يرسو عليه العطاء

للإستفسار هاتف 5600230 فرعي (2531 / 2009)

بسـم الله الـرحمـــن الـرحيـم

جامعة العلوم الإسلامية العالمية

لجنة العطاءات المركزية

رقم العطاء : 2022/7

التـــاريـــخ :

المتعهد .....المحترم

تحتاج جامعة العلوم الإسلامية العالمية إلى اللوازم / أو الأشغال المبينة تفاصيلها فيما هو مرفق ،يرجى تقديم عرضكم لتوريد هذه اللوازم وفق التعليمات والشروط العامة والخاصة والمواصفات الفنية المرفقة بهذا العطاء .

هذا ويشترط للنظر في عرضكم ، أن يقدم على النموذج المرفق وأية نماذج عروض اسعار اخرى على ورق المتعهد ولا يقبل العرض الذي يقدم بعد التاريخ المحدد بتقديم العروض، ويستبعد أي عرض لا يكون موقعا من مقدمه او وكيله القانوني بموجب وكالة ترفق بالعرض وذلك تحت طائلة رفضة.

واقبلوا فائق الاحترام والتقدير

رئيس لجنة العطاءات المركزية

جامعة العلوم الإسلامية العالمية

ملاحظة : تقدم الأسعار على أساس أنها شاملة للضريبة العامة على المبيعات ؛ لكون الجامعة غير معفاة منها .

بسـم الله الـرحمـــن الـرحيـم

جامعة العلوم الإسلامية العالمية

لجنة العطاءات المركزية

رقم العطاء :2022/7

التـــاريـــخ :

(نمـــوذج عـــــرض مناقصة)

رئيس لجنة العطاءات المركزية / جامعة العلوم الإسلامية العالمية

بناء على دعوة العطاء رقم (2022/7) ووفقاً للتعليمات و الشروط العامة والخاصة والمواصفات الفنية والملاحق المرفقة، فإنني

أقدم عرضي وأوافق على أن أقوم بتوريد اللوازم المعروضة أو أجزاء منها بالأسعار وشروط التسليم والمواصفات الواردة في هذا العرض .

السـعر الاجمـالي للعطـاء :.....شـاملا الضـريبة العامة على المبيعات وحسب الكشف التفصيلي المرفق .

أرفق طيه التأمين المطلوب (كفالة دخول العطاء) بقيمة (.....) (.....) دينار أردني ، بموجب (كفالة بنكية / أو شيك مصدق) رقم ..... صادرة عن/ أو مسحوب على بنك ..... .

ونؤكد أنكم غير ملزمين بإحالة العطاء على أقل الأسعار كما نعلمكم بأننا قد دفعنا قيمة نسخة العطاء المقررة وهي غير مستردة بموجب إيصال المقبوضات (مرفق نسخة منه) رقم (.....) تاريخ (/ /) .

و إنني ألتزم بأن يبقى العرض ساري المفعول لمدة (120) مائة وعشرون يوماً ابتداءً من تاريخ (/ /) .

اسم المفوض بالتوقيع : ..... الوظيفة : .....

التـــــــوقيـــع : ..... رقم الخلوي : .....

اسـم المناقص : ..... العنوان : .....

هـــــاتـــــــف : (.....) ص . ب . (.....) فـــاكـــس : (.....)

البريد الإلكتروني : (.....)

الختـــم الـرسمـــي :

جامعة العلوم الاسلامية العالمية

لـجـنـة الـعـطـاءات الـمـركـزيـة

نموذج كشف مفصل لتحليل الأسعار المقدمة مع عرض المناقصة

عطاء رقم (2022/7)

الرقم	البيـــان	السعر الإفرادي		الكمية		المبلغ الاجمالي	
		فلس	دينار	العدد	الوحده	فلس	دينار
1							
	المبلغ الإجمالي كتابة :						

الرقم الضريبي (.....) وإذا لم يكتب يكون خاضع للضريبة، علماً أن السعر شاملاً الضريبة العامة على المبيعات وأية ضرائب أو رسوم أخرى تترتب على هذا العطاء إذا استحقت لاحقاً ولا يحق له المطالبة بها .

اسم المفوض بالتوقيع :..... الوظيفة :.....

التوقيع:..... ..... رقم الخلوي :.....

اسم المناقص:.....العنوان : .....

هاتف: (.....) ص.ب. (.....) فاكس: (.....)

البريد الإلكتروني : (.....)

الختم الرسمي :

جامعة العلوم الإسلامية العالمية

لجنة العطاءات المركزية

دعوة عطاء رقم : (2022/7)

"نظام حماية الأجهزة الطرفية "

الشروط العامة والخاصة

الشروط العامة

أولاً : أ : يقدم العرض على النموذج المقرر أو مكتوباً بالحبر بخط واضح خالٍ من المحو أو التعديل أو الشطب إلا لضرورة ذلك، وعندها على المناقص التوقيع بجانب المحو أو التعديل أو الإضافة وعليه كتابة السعر بالرقم والحروف . وعلى المناقص كذلك أن يذكر السعر الإفرادي للوحدة الواحدة وسعر المادة بكامل وحداتها وكذلك السعر الإجمالي للعرض(لجميع المواد المقدم لها)، وبخلاف ذلك يحق للجنة العطاءات أن تهمل العرض .

ب : لا تقبل العروض غير الموقعة وغير المختومة من مقدميها ، أو من وكلائهم حسب الأصول أو التي ترد ناقصة أو غامضة بشكل لا يمكن من الإحالة .

ج : لا يجوز إدخال أي تعديل أو إجراء أي تبديل في نموذج العرض للمناقصة أو أي من وثائق المناقصة المرفقة به من قبل المناقص باستثناء تعبئة المواقع المطلوب تعبئتها و إذا أجرى المناقص أياً من تلك التعديلات أو التبديلات أو إذا أخل بأي من هذه التعليمات ، يحق للجنة إهمال عرضه . وإذا أراد المناقص وضع بعض الشروط أو التحفظات أو البدائل التي تناسبه فان باستطاعته تضمين ذلك في مذكرة خاصة منفصلة ترفق بالعرض .

د : على المناقص - عندما يطلب منه ذلك - تقديم البيانات و الوثائق الأصلية التي تثبت خبرته ومقدرته الفنية والمالية ودرجة الخدمة المتوفرة لديه وأي متطلبات أخرى ضرورية تدل على قدرته على الوفاء بكل ما يتعلق بالعطاء من التزامات ومتطلبات .

هـ : يقدم العرض على نسختين مرفقة بكافة وثائق دعوة العطاء مختمة من قبل المناقص (أصلية + صورة) مع مراعاة ضرورة تعبئة نموذج عرض المناقصة وتوقيعه حسب الاصول كما ذكر في البند (أ) من الشروط العامة توضع كل نسخة في مغلف منفصل وترفق بالمغلف الذي

يحتوي التأمين الخاص بدخول العطاء وتضمن المغلفات الثلاثة في مغلف مغلق بإحكام ،ومختوم ومعنون باسم (لجنة العطاءات المركزية / جامعة العلوم الإسلامية العالمية) ومكتوب عليه بخط واضح اسم المناقص وعنوانه ورقم دعوة العطاء ونوع اللوازم والأشغال والتاريخ المحدد كآخر موعد لتقديم العروض، وبخلاف ذلك يحق للجنة العطاءات أن تهمل العرض .

و : يودع العرض من قبل المناقص في صندوق العطاءات لدى إدارة الجامعة قبل انتهاء المدة المحددة لذلك ويفضل أن تكون قبل آخر موعد بفترة كافيه تجنباً لأي طارئ وكل عرض لا يصل ولا يتم إيداعه في صندوق العطاءات قبل آخر موعد لتقديم العروض ، فلن ينظر فيه ويعاد إلى مصدره مغلقًا ، وفي حالة عدم كتابة عنوان المرسل أو المعلومات الكافية الواضحة عن العطاء فيحق للجامعة فتحه لمعرفة محتويات المغلف والعنوان إن وجد لإعادته .

ثانياً : على المناقص أن يبين في عرضه عنواناً ثابتا ترسل إليه جميع المراسلات المتعلقة بالعطاء، وعليه أن يبلغ اللجنة بكتاب مسجل عن أي تغيير أو تعديل في عنوانه وإلا فإنها لن تكون ملزمة بمراعاة هذا التغيير أو التعديل ، وتعد جميع المراسلات التي تترك في العنوان المذكور أو ترسل إليه بالبريد كأنها وصلت فعلا وسلمت في حينها .

ثالثاً :

أ : على المناقص أن يقدم أسعاره رقماً وكتابةً على النموذج المخصص لذلك ، ويرفض أي عرض يحدث فيه المناقص تشويشًا في أسعاره، واللجنة غير مسؤولة عن أي أخطاء قد يرتكبها المناقص في وضع الأسعار .

ب : لا تلتزم الجامعة بتعويض المناقص عن أي فرق في السعر ينجم عن التغير في الاسعار و/أو التكاليف طوال مدة العطاء .

رابعاً : يعد عرض المناقص تأكيداً منه أن عرضه لم يقدم بناء على علاقة مع مناقص آخر تقدم لمادة أو أكثر من المواد الواردة في عرضه، وفي جميع الأحوال لا يجوز لمناقص واحد أن يقدم عرضين مستقلين لنفس اللوازم سواء كان باسمه الشخصي أو بشراكته مع اسم آخر وفي هذه الحالة لا ينظر في العرضين ، وعلى المناقص أن يقدم عرضًا واحدًا محددًا ، ويجوز للمناقص أن يرفق مع عرضه بعض البدائل الاختيارية بوثائق مستقلة ، على أن تتناسب قيمة تأمين الدخول في العطاء مع قيمة العرض أو البديل أيهما أعلى .

خامسًا : أ : على المناقص أن يرفق بالعرض ،لصالح جامعة العلوم الإسلامية العالمية ولأمرها ، تأمينا للدخول في العطاء (Bid Bond)كفالة مصرفية أو شيكاً مصدقاً من قبل أحد المصارف المحلية لا يقل عن(3%) ثلاثة بالمئة من قيمة عرضه وأن يكون صالحًا لمدة (120) مائة وعشرون يوماً من تاريخ آخر موعد لاستلام العروض ولا ينظر في العروض غير المعززة بتلك التأمينات بحيث يلتزم المناقص بان يكون تجديد الكفالة المقدمة تلقائيا

ب : يقدم المناقص الذي يحال عليه العطاء تأمينا لحسن التنفيذ (Performance Bond) بنسبة (10 %) عشرة بالمئة من قيمة العطاء أو المواد المحالة عليه لأمر جامعة العلوم الإسلامية العالمية على صورة كفالة مصرفية أو شيك مصدق من قبل أحد المصارف المحلية تبقى سارية المفعول لحين تسليم اللوازم أو الأشغال بحيث يلتزم المناقص بان تجديد الكفالة المقدمة تلقائية، ويحفظ هذا التأمين لدى دائرة الشؤون المالية في الجامعة كضمان لتأمين تنفيذ العقد على الوجه الأكمل ، ولاستيفاء ما تم دفعه زيادة على المبالغ الواجب دفعها ، وكذلك لاستيفاء الغرامات والتعويضات وفروق الأسعار أو التكاليف التي تستحق لحين الانتهاء من تنفيذ العقود .

سادسًا : لا تنظر لجنة العطاءات المركزية بأي عرض يُقَدم على غير النسخ التي تم شراؤها للعطاء . و أن يتم توقيع أي ملحقات و/أو مرفقات و/أو كشوفات و/أو جداول من قبل المفوض الرسمي حسب الرخص و السجلات التجارية الرسمية وإرفاق صورة عن إثبات الهوية الشخصية له ويرفق معها كشف بالخدمات أو العطاءات السابقة التي شارك في تنفيذها للمؤسسات العامة أو الخاصة معززة بشهادات رسمية تثبت حسن الأداء لها .

سابعاً :

أ : تحسب مدة التسليم ابتداءً من تاريخ التوقيع على قرار الإحالة، وتعرف مدة التسليم بأنها مجموع الأيام أو الأشهر التقويمية وتكون شاملة لأيام العطل والجمع والأعياد الرسمية.

ب : تحسب غرامات التأخير على أساس (0.002) اثنان بالألف من قيمة العطاء عن كل يوم تأخير وبحد أقصى (15%) من القيمة الإجمالية للإحالة، وتحسم الغرامة من المبالغ المستحقة للمتعهد وإذا وافقت الجامعة على تسلم أي أجزاء من

العطاء بشكل يتيح لها استعمالها واستغلالها فيمكن عندها تخفيض غرامة التأخير بنسبة قيمة اللوازم / الأشغال التي تم تسليمها من أصل العطاء .

ثامناً : يلتزم المناقص بأسعاره لمدة (120) مائة وعشرون يومًا من تاريخ اخر موعد لاستلام العروض، ويعد توقيعه على (نموذج عرض المناقصة) التزامًا بذلك .

تاسعاً : ترفق بالمناقصات صورة عن رخص المهن والسجل التجاري وشهادة تسجيل للشركة و/أو للمؤسسة (سارية المفعول) .

عاشرًا : تحتفظ اللجنة لنفسها بحق استبعاد أي عرض لا يكون واضحاً بصورة كافية أو يحتمل أكثر من تفسير أو إذا كان ناقصًا في بيان مواصفات مواد العطاء أو الشروط والمواعيد الخاصة بتسليمها أو لم يقدم على النموذج المقرر المرفق بدعوة العطاء

حادي عشر : يجوز للمناقص سحب عرضه بمذكرة موقعة منه تودع في صندوق العطاءات قبل الموعد المحدد بيوم عمل واحد على الأقل لفتح العطاء .

ثاني عشر: تقبل اللجنة أي تعديل في الأسعار الواردة في العرض يصلها بمذكرة تودع في صندوق العطاءات قبل الموعد المحدد بيوم عمل واحد على الأقل لفتح العطاء .

ثالث عشر: اللجنة غير مقيدة **باقل** الأسعار، ولها الحق في تجزئة العطاء أو إلغائه كليًا أو جزئيًا إذا اقتضت مصلحة الجامعة ذلك ،دون أن يكون لأي من المناقصين الحق في المطالبة بأي خسارة أو ضرر ناتج عن ذلك .

رابع عشر: إذا وجدت اللجنة أن الأسعار المقدمة مرتفعة أو لا تتناسب مع التقديرات الموضوعة لتلك اللوازم أو الأشغال ، او العروض التي وردت غير مقبولة او العروض غير مكتملة وتعذر اكمالها ، فلها أن تقوم بأي من الإجراءات التالية حسبما تراه مناسبا لمصلحة الجامعة: -

أ : التفاوض مع مقدم أرخص الأسعار؛ لتخفيضها إلى المقدار الذي تراه مناسبا .

ب : إلغاء العطاء والتفاوض مع الذين اشتركوا فيه ومع غيرهم للحصول على سعر أقل وتلزيم اللوازم أو الأشغال بموجبه .

ج : إعادة طرح العطاء .

خامس عشر : إذا وجد في أي من العروض المقدمة نقص، أو خطأ أو تناقض بين حساب جملة أي مبلغ، وما يجب أن تكون عليه هذه الجملة بتطبيق السعر الموضوع لأي بند في جدول الكميات، فللجنة الحق في تعديل جملة المبلغ بما يتفق وتطبيق السعر الموضوع على الكمية الموضوعة لذلك البند. وبالتالي تعديل مجموع السعر أو المبلغ

المقدم للعطاء ، وإذا حدث خلاف بين العدد المذكور بالأرقام والمذكور كتابة فتعد الكتابة هي الملزمة، وكذلك إذا حدث خطأ في جمع قيمة مختلف البنود فإن للجنة الحق في تصحيح المجموع ويكون المجموع المصحح في مثل هذا العطاء هو الملزم للمناقص .

سادس عشر :

أ : يوقع الشخص الذي أحيل عليه أي عطاء اتفاقية / أو عقد لتنفيذ الأعمال المطلوبة وفقاً للشروط والمواصفات المقررةللوازم والمواد المكتبية و الأشغال المطلوبة في العطاء ، على أن ينص في الإتفاقية و / أو العقد على أن تلك الشروط والمواصفات والأمور الأخرى الواردة في دعوة العطاء وفي الوثائق والمخططات المرفقة أو الملحقة به تعد جزءًا من تلك الإتفاقية / أو العقد .

ب : لا يجوز للمناقص الذي أحيل عليه أي عطاء للجامعة أن يتنازل عنه أو عن أي جزء منه إلى أي شخص آخر بأي صورة من الصور بدون موافقة خطية من اللجنة ووفقاً للشروط والضمانات التي تقررها، على أن تصدق موافقة اللجنة من قبل الجهة التي سبق لها وصدقت على قرار الإحالة .

سابع عشر : إذا لم يقم المناقص الذي أحيل عليه العطاء بعد تبليغه قرار إحالته عليه بتوقيع اتفاقية /أو عقد تنفيذ العطاء، وتقديم الكفالات والتأمينات المطلوبة منه خلال عشرة أيام من تاريخ تبليغه قرار الإحالة فيعد مستنكفًا عن تنفيذ العطاء ويصادر مبلغ الكفالة أو التأمين الذي قدمه عند اشتراكه في العطاء ، وللجنة في هذه الحالة إما إحالة العطاء على مقدم العرض الأرخص بعد العرض الذي قدمه المستنكف ، أو إلغاء العطاء وإعادة طرحه، وتضمين المتعهد المستنكف في الحالتين فرق السعر وأي مبالغ أو أضرار أخرى تلحق بالجامعة نتيجة استنكافه وحرمان المتعهد المستنكف أو المتخلف من الاشتراك في أي عطاء أو أعمال للجامعة للمدة التي تقررها اللجنة على أن لا تقل عن ستة أشهر.

ثامن عشر :

أ : إذا تخلف المتعهد عن تنفيذ العطاء الذي أحيل عليه كليا أو جزئيا أو خالف أي شرط من شروط العقد ، فللجنة اتخاذ إجراء من الإجراءات التالية أو أكثر بحقه :

1 : مصادرة جزء أو كل مبلغ الكفالة أو التأمين الذي قدمه ذلك المتعهد ضماناً لحسن التنفيذ وقيده إيراداً للجامعة .

2 : تنفيذ العطاء بالشروط والطريقة التي تراها مناسبة ، وتحميل المتعهد أي فرق في الأسعار مضافًا إليه (15%) من ذلك الفرق نفقات إدارية ، إضافة إلى أي نفقات مباشرة وغير مباشرة تتحملها الجامعة وإذا لم يكن هناك فرق في الأسعار يتحمل المتعهد(10%) سعر اللوازم أو أوعية المعلومات أو الأشغال التي تخلف عن توريدها أو تنفيذها يضاف إليها أي نفقات مباشرة أو غير مباشرة تحملتها الجامعة .

ب : تتخذ اللجنة أي إجراء من الإجراءات المنصوص عليها في الفقرة (أ) من هذه المادة أو أياً من الإجراءات المنصوص عليها في المادة (34) من هذا النظام ، دون أن تكون ملزمة بتوجيه أي إخطار أو إنذار إلى المتعهد المستنكف أو المتخلف قبل تنفيذ تلك الإجراءات .

تاسع عشر : يدفع المتعهد المحال عليه العطاء، الطوابع القانونية ورسوم الإحالة ورسوم العقود والرسوم الإضافية وأي رسوم أخرى مستحقة بموجب القوانين والأنظمة المعمول بها، ويتم تسديد هذه الرسوم والطوابع عند التوقيع على قرار الإحالة .

عشرون : أجور الاعلانات الخاصة بالعطاء على من يرسو عليه العطاء ومهما بلغت عدد مرات الاعلانات .

واحد وعشرون : يتنازل المتعهد ويسقط حقه ويعفي الجامعة/لجنة العطاءات المركزية من توجيه الإنذارات والإخطارات العدلية .

اثنان وعشرون : في حال نشوء أي نزاع يتعلق بتنفيذ بنود هذا القرار أياً كان نوعه فإنه على المتعهد إشعار الجامعة بوجود مثل هذا النزاع ، وعلى الفريقين بذل جهودهما القصوى لحل النزاع وديًا قبل أن يتم اللجوء إلى القضاء وفي حال اللجوء للقضاء يكون الاختصاص المكاني لمحكمة شرق عمان حصرًا .

ثلاثة وعشرون : إن شروط دعوة العطاء والشروط العامة والخاصة والتعليمات تعتبر جزءاً لا يتجزأ من قرار الإحالة مع الأخذ بعين الاعتبار التعديلات الموافق عليها مسبقاً من قبل لجنة العطاءات المركزية حيث تعتبر هذه التعديلات جزءًا مكملًا لقرار الإحالة وملحقاته حسب الأصول .

أربعة وعشرون : يحق للمناقصين الذين قاموا بشراء نسخة العطاء في المرة الأولى الحصول على نسخة عطاء مجانًا في حال إعادة طرحة " للمرة الثانية " .

خمسة وعشرون : لا يقبل العرض الذي يقدم بعد التاريخ المحدد لتقديم العروض ويستبعد أي عرض لا يكون موقعاً من مقدمه أو وكيلة القانوني بموجب وكالة ترفق بالعرض وذلك تحت طائلة رفضه.

ستة وعشرون : اذا وجد أي تعارض بدعوة العطاء و/أو الإحالة و/أو العقد المبرم مع الجامعة فللجنة العطاءات المركزية الحق بإتخاذ القرار أو الإجراء المناسب بما يصب ويتناسب مع مصلحة الجامعة

سبعة وعشرون : إن دعوة العطاء والشروط العامة والخاصة والمواصفات الفنية هي جزء لا يتجزأ من دعوة العطاء .

ثمانية وعشرون : يعتبر نظام اللوازم والأشغال رقم (15) لسنة (2018) والشروط العامة والخاصة والمواصفات الفنية و الملاحق والكشوف والجداول المرفقة بدعوة العطاء جزءاً لا يتجزأ من قرار الإحالة بالإضافة إلى العرض المقدم من المتعهد .

عدد صفحات دعوة عطاء رقم (2022/7) والخاص ب" نظام حماية الأجهزة الطرفية " بما فيها الشروط العامة والخاصة والمواصفات الفنية (17) صفحة بحيث يتوجب على مندوب الشركة التأكد من عددها كاملاً قبل مغادرة الدائرة .

المواصفات الفنية لنظام حماية الاجهزة الطرفية

1. تلتزم الشركة المنفذة بالدعم الفني للجامعة طيلة فترة التعاقد على مدار الساعة (7/24) على ان يكون الدعم الفني المقدم من الشركة المنتجة موجودا بجميع الاحوال على طول فترة الصيانة.
2. يتم احتساب التراخيص من لحظة الاستلام النهائي و ليس من لحظة التوريد.
3. المورد يجب أن يكون من أصحاب الخبرة ومن مستوى مصرح له في البيع من الشركة الام، ويفضل أن يكون حاصل على اعلى درجة تمثيل (Partnership) من الشركة الام ، و تقديم شهادة التمثيل على ان تكون سارية المفعول.
4. يجب أن يكون لدى المورد مهندسين اثنين على الاقل ممن يحملون شهادات فنية من الشركة الام التي تثبت كفاءتهم وقدرتهم على تشغيل وتفعيل البرمجيات و يشترط على الشركة تزويد الجامعة بنسخ من الشهادات المطلوبة و السيرة الذاتية للكادر.
5. يجب على المورد خلال فترة التنزيل ان يقوم بتوضيح كافه المعلومات وآلية التنصيب لمهندسي الجامعة .
6. المورد يجب ان يقدم تدريب كامل (المعتمد من الشركة الام) على استخدام البرمجيات (official Training) لموظفين عدد (2).
7. إرفاق شهادات خبرة للأعمال المنجزة من المورد في العطاء المذكور ، على ان تكون الخبرات في مشاريع مشابهه.
8. يشترط على الشركة المموردة الاخذ بعين الاعتبار شروط التنفيذ والاستلام الموضحة ادناه في الشروط الفنية
9. يشترط على ان لا تقل صلاحية العرض المقدم عن 120 يوم .
10. يجب على المشاركين بالعطاء تسليم نسخة الكترونية اضافة للنسخ الاخرى الورقية المطلوبة.
11. يحق للجامعة عند الاستلام فحص الانظمة و عمل فحوصات اختراقات بحيث تضمن فعالية البرمجيات المستخدمة (سواء عن طريق الجامعة او اي طرف ثالث ترتئيه الجامعة).

Security Functionality for the EndPoint

Centralized Management Console

1. WISE need **one single management console** to **fully manage and configure** the following security services "Endpoint Protection (EPP), EDR."
2. The EDR and Endpoint protection should support full (EPP, EDR, Device Control ,Sandboxing , vulnerability detection, web filtering, Host based FW)
3. Approved EDR and EPP for the tender:
    1. Fireye
    2. VMWARE (carbon black)
    3. Cisco
    4. BitDefender
    5. Broadcom (Symantec)
    6. PaloAlto
    7. Fortinet
    8. Microsoft Defender
4. The scope should cover 750 Devices and the offer should provide 1- and 3-years renewal options.
5. The Awarded party shall manage the implementation end to end.
6. Since current WISE AV (Kaspersky) licenses will be expired in 17/7/2022 , then the winning party shall provide immediate license that cover the university till final implementation is done.
7. Bidder shall have the required team certificate for implementing the solution.
8. The management console should support Two-Factor Authentication
9. The management console might be delivered and fully operated on-premises or Cloud
10. The management console should support role-based access control for administrators.
11. The product should allow automatic offline machine cleanup based on rules defined by administrators.
12. For easy deployment, a single Remote deployment task should be used for deploying the security agent on Windows, Linux instead of using multiple deployment tasks based on OS type.
13. Ability to uninstall the existing third-party antimalware product during the deployment task.
14. The Solution must provide Agents to do the following tasks on behalf of the Management Server:
    a. Network Discovery.
    b. Distribution point of Updates and missed patches.
    c. Patch Management Cache Server.
15. Capability to assign a policy to a single selected endpoint or multiple selected endpoints.
16. Capability to assign a policy to a group of endpoints that can belong to a specific custom group or AD Organizational Unit.
17. For easy management, a single policy can be configured and applied on security agents installed on Windows, and Linux operating systems.
18. The Vendor shall provide minimum HW specs for machines were Agent will be install.

NextGen Endpoint Protection & EDR

1. The existence of a single endpoint protection agent offers NextGen EPP + EDR features.
2. The Security agent must support Windows, Linux operating systems.

3. Instead of using another Network agent, The Endpoint Protection Security agent must come with built-in communication module to communicate with its management console without any need for additional agents to be installed.
4. The single protection agent must come with the following all in one protection layers:
    a. Anti-Malware
    b. Advanced Anti-Exploit
    c. Anti-Ransomware “with ransomware activity rollback”
    d. Anti-Phishing
    e. Web Traffic Scan
    f. Tunable Machine Learning
    g. File-less Attack Protection
    h. Process Inspector “behavioral analysis”
    i. Local & Cloud Machine Learning
    j. Sandbox Analyzer
    k. Firewall & IDS
    l. Network Attack Defense
    m. Endpoint Detection & Response “EDR”
    n. Application Control, Device Control, Web Access Control
5. To minimize resource consumption, the product must allow custom modules installation (e.g., installing the antimalware product without the web access control module or without Firewall module).
6. The solution should provide ability to add or remove any protection module of already installed EPP agent by remote reconfiguration task without reinstalling the Agent.
7. Supported operating systems:
a. **Windows:** Win 7, 8/8.1, 10, 11, 2008 R2, 2012, 2012 R2, 2016, 2019 and 2022 (vendor should state if windows XP and 2003 is supported)
b. **Linux:** Red Hat Enterprise Linux / CentOS 6 or higher, Ubuntu 14.04 LTS or higher, SUSE Linux Enterprise Server 11 SP4 or higher, OpenSUSE LEAP 42.x or higher, Fedora 25 or higher, Debian 8.0 or higher, Oracle Linux 6.3 or higher, IBM AIX
8. For greater protection, antimalware should have 5 types of detection: signature-based, heuristic based, machine learning, process inspector “behavioral analysis” and cloud analysis.
9. The solution must provide ransomware mitigation module for real time back-up of the files before being modified by suspicious processes to mitigate the risk of losing data during advanced ransomware attacks.
10. The ransomware mitigation module should detect ransomware families in zero-day based on behavioral analysis and machine learning.
11. The ransomware mitigation module should automatically recover files encrypted by ransomware upon detection.
12. The solution must include machine learning algorithms used against zero-day or advanced exploit (directional) attacks.
13. The Solution must provide an additional next-generation security layer, based on aggressive heuristics and tunable machine learning technology, to detect and block the new generation of advanced or targeted attacks and sophisticated malware before execution. It must provide:
    a. Classification of the attack types.
    b. Ability to only report detected threats, without blocking them.
    c. Ability to adjust the detection aggressiveness for each attack category, with options to act on higher confidence detections and report all other lower confidence detections. At least 3 detection levels should be available.

d. Ability to take different actions on detected files and network-based threats.

14. Ability to detect file-less attacks, including those making use of legitimate operating system tools such as PowerShell or script interpreters and the solution shall not globally block scripts to achieve this.
15. The solution must offer behavioral analysis which continuously monitoring of all running process to detect and terminate advanced threat on execution
16. The solution must provide the ability to automatically rollback all malicious activities upon detection.
17. The solution must offer advanced anti-exploit protection layer to stop zero-day attacks by real-time detection of the most recent exploits that can be used to gain privileges over an operating system.
18. For greater protection, antimalware must be able to scan HTTP and SSL as well.
19. The Solution must provide network attack protection layer which will protect from network-based attacks like “lateral movement, brute force attacks, credential access, network exploits, password stealers, network discovery, ...etc”.
20. EDR solution must allow query to all the host endpoints in enterprise for specific indicators of compromise (IOCs).
21. EDR solution must detect exploitation in MS word, MS excel, MS PowerPoint, Java, Flash, IE, Firefox, and Chrome,.. etc.
22. The Network attack protection must inspect all network traffic in both directions (incoming and outgoing).
23. The solution must offer Firewall layer providing the following features:
    a. ability to set the "stealth mode" in LAN and internet.
    b. The module can be installed/uninstalled according to the administrator’s preferences.
    c. Ability to define trusted networks for a specific endpoint / group of endpoints.
    d. The ability to detect Port Scans.
    e. The ability to set different Network Profiles (Home/Office, Trusted, Public, Untrusted or Let the Windows decide) for specific networks or for adapters (Wired, Wireless, Virtual)
    f. Ability to create custom rules based on Application and/or Connection.
24. The Endpoint protection agent must come with protection password
25. The antimalware product must contain a scanning engine and it must be able to run scheduled scans and can automatically shut down after scanning the workstation.
26. For best performance, the antimalware product must work with low CPU priority.
27. The solution should provide Built-in Exclusions for Microsoft Server Roles (DNS, DHCP, AD, Exchange, SharePoint …).
28. Ability to define an exclusion list from scanning for **folders, files, paths, file extensions, processes, threat name**. Scan exclusions should support wildcards.
29. Ability to define an exclusion list from scanning for **certificate hash and command line**
30. The endpoint security agent must include a sandbox analyzer module to integrate with the provider sandbox and automatically submit samples for detonation.
31. The endpoint security agent should deny access to detonated samples until receiving the Sandbox analysis result.
32. The endpoint security agent must be able to automatically remediate malicious detonated samples by the sandbox analysis.

33. The solution must offer application control with Whitelisting/Blacklisting capabilities.
34. The solution must offer web access control as a web filtering to control user's internet web access
35. and device control features to block any plug and play devices like "external storage, Modems, etc."
36. The Solution must provide application whitelisting/blacklisting, in addition to application inventory.
37. The solution must provide user content control module with the following features:
    a. Blocking Internet access for specific clients or client groups.
    b. Blocking access to certain applications.
    c. Blocking Internet access for certain periods of time.
    d. Block web pages that contain certain keywords or category.
    e. Allow access to specific web pages specified by the administrator.
38. The solution must include an "Endpoint Detection and Response - EDR" module able to identify advanced attacks that are taking place in realtime (execution phase).
39. The EDR Module must be covered by **the same Endpoint Protection bundle license**, no additional license is required.
40. The EDR module should offer both automatic and manual threat hunting capabilities.
41. The EDR module must have the ability to evaluate typical endpoint activity (baseline) according to MITRE techniques and report any deviation from typical activity by generating a new incident in the management console.
42. The EDR module allows for visualization "incident graph" in great details for each incident including specific details for each affected endpoint, specific process and incident timeline.
43. The EDR module must have the ability to act on every step of the incident with a set of actions that can be used to further investigate (sandbox, virus total, google search).
44. The EDR module must have the ability to simply kill the process, quarantine files, add to blocklist, isolate the host, remote connect to isolated hosts, install patches, or add an url exception (depending on the type of threat evaluated at each step of the incident).
45. The EDR module can block files and/or processes based on hash values (MD5/SHA256) added directly by administrator to the management console or imported them via a .csv file.
46. The EDR module should allow administrator to set custom behavioral detection rules.
47. The EDR module should provide response and forensics investigations mechanisms like
    a. Live remote shell from the console to any Endpoint
    b. Support for file upload/download
    c. Process memory dump generation.
48. The solution includes a host IPS module able to block various network-layer threats including the prevention of lateral movement for various categories of malware.
49. The host IPS module is integrated with the EDR module and the later can include specific information from the host IPS module in the incident details.
50. Optionally, WISE need to push notification messages to end users using the agent installed

Reporting and Dashboard :

1. The solution should report in-depth on system-level OS and application changes to file system
2. The solution should support reporting in HTML/Graphical/CVS/PDF Formats
3. The solution should provide ability to report incidents per user, computer, application , attack, file, or IOC
4. The solution should support daily/weekly/monthly reporting
5. The solution should support Easy to use from one view: summary and details in the same page.
6. For reporting the solution should have as Scheduled, that can be sent by mail to any number of recipients (it's not required to have also an account in the console).
7. The solution should allow the visualization of reports that are currently being generated by the administrator.
8. The solution should support the Export of reports to .pdf file, details to .csv file.
9. The solution should support report customization to aggregate events from any security module into a single report based on multiple criteria as follows: endpoint status, endpoint events, Events.
10. Endpoint status reports include the following (not limited to) info:
    a. Workstation type
    b. Workstation network
    c. Endpoint client details
    d. Security signature details
    e. Workstation role
11. Endpoint events reports include the following (not limited to) info:
    a. The workstation where the event took place
    b. The type, state and configuration of the endpoint client
    c. The name and status of the policy currently enforced on the endpoint
    d. The user that was logged on during the event
    e. Other criteria (blocked website, malware detection, etc)