عطاء رقم (2026/20)

شراء نظام الكشف والاستجابة للتهديدات السيبرانية NDR

فهـــــرس

==========

دعوة العطـــــــــــــــــاء

صيغـة العقـــــــــــــــــد

الملحـــــــــــــــــــــق

نمـوذج كفالة دخول العطـــــــاء

نمـوذج كفالة حسن تنفيـــــــــذ

نمـوذج كفالة الصيانـــــــــــة

تعليمات عامــه للمشتركيـــــــن

الشروط العامـــــــــــــــة

الاسعـــــــار والدفـــــــــع

المواصفات الفنية الشـروط الخاصـة

دعوة العطاء

شركة الكهرباء الوطنية

العطاء رقم 20/ 2026

تدعو شركة الكهرباء الوطنية السادة المتعهدين لتقديم عروضهم باللغة العربية أو الإنجليزية للعطاء في الجداول المرفقة بناءً على التعليمات والشروط العامة والخاصة الموضحة بوثائق العطاء على النماذج المقررة لذلك.

على المتعهدين تعبئة نموذج العطاء والجداول المرفقة وتقديم الوثائق كاملة وموقعه على كل صفحه حسب الأصول الكترونياً من خلال الموقع الإلكتروني www.joneps.gov.jo في موعد أقصاه الساعة الثانية من بعد ظهر يوم الأحد الموافق 2026/04/19

صيغـة العقـد

مدير عام شركة الكهرباء الوطنية

ص.ب. (2310)

عمان – الاردن

تحيه وبعد،،،

1- بنـاء علـى دعـوة العطـاء رقـم 20 / 2026 وبعد الاطـلاع علـى الشـروط والمواصـفات والجـداول نتعهـد نحـن الموقعون أدناه بتوريد وتنفيذ الأعمال المطلوبة وذلك حسب المواصفات والشروط والتعليمات العامـة المـذكورة فـي العطاء أعلاه وفقاً للأسعار المبينة في عرضنا.

2- في حالة قبول عرضنا نتعهد ببدء العمل حال استلامنا لأمر الشراء اللازم على ان يتم البدء بالعمل خـلال فترة –

--------- من تاريخ الإبلاغ.

3- نبين فيما يلي الرقم الوطني الضريبي هو ( ).

التاريـــــخ : .....

التوقيـــــع : .....

المخول بالتوقيع نيابه عـن : .....

العنـــــوان :.....

المهنـــــة : .....

الملحـــق
(Appendix)

* يعتبر هذا الملحق جزءاً من وثيقة العطاء

المـادة	الموضـوع	البيـــان
	المواصفات	المواصفات الفنية العامة والخاصة
	المخططات	ان وجدت
	ثمن الوثيقة	125 دينار اردني
	كفالة الدخول	6000 دينار اردني على أن تكون إما كفالة بنكيه أو شيك مصدق صادر عن بنك محلي سارية المفعول لمدة (90) يوماً تقويمياً ابتداء من تاريخ إغلاق العطاء
	صلاحية العروض	90 يوم
	أولوية الوثائق	1- الاحالة 2- الشروط الخاصة. 3- الشروط العامة. 4- المواصفات. 5- المخططات (إن وجد). 6- جداول الكميات.
	القانون الذي يحكم العطاء	القانون الأردني
	مكان التسليم	المكاتب الرئيسية
	عملة عروض الأسعار	الدينار الأردني
	ضمان الأداء (كفالة التنفيذ) - القيمة	يطلب منكم تقديم كفالة حسن تنفيذ بنسبة (10%) من قيمة الإحالة الكلية تقدم خلال مدة 28 يوم من تاريخ تبليغكم قرار الإحالة.
	كفالة إصلاح العيوب (كفالة الصيانة)	(5%) من قيمة الإحالة ولمدة ثلاث سنوات من تاريخ الاستلام الفعلي للمواد وإنجاز الاعمال.
	غرامات التأخير - القيمة - الحد الأقصى	عندما يتأخر المتعهد عن تنفيذ ما التزم به في الموعد المحدد في العقب فللشركة أن تفرض عليه جزءاً مادياً بصرف النظر عن الضرر الناشيء عن التأخير في التنفيذ لا يتجاوز ½% من قيمة المواد التي تأخر في تسليمها عن كل أسبوع أو جزء من الأسبوع. (15)% من قيمة الإحالة الاجمالية.

كفالة دخول في العطاء رقم : .....

بنك : .....

كفالة رقم : .....

استحقاق : .....

السادة شركة الكهرباء الوطنية

عطاء رقم (2026/20)

_____

نرجو العلم بنك .....

يكفل لأمركم السيد / السادة .....

مبلغ وقدرة ..... وذلك لقبول عرضه المقدم لتنفيذ العطاء المشار اليه أعلاه.

تبقى هذه الكفالة سارية المفعول لمدة ..... بعد التاريخ المحدد لفتح العطاء المذكور، وهي قابلة للتمديد بناء على طلبكم ولا يترتب عليكم أية فوائد بخصوص هذه الكفالة، ونتعهد بدفع قيمتها لكم عند الطلب دون أي تأخير أو ممانعة ودون الحاجة لأي إنذار أو مطالبة قضائية.

واقبلوا الإحترام ,,,,

بنك .....

كفالة حسن تنفيذ

البنك او المؤسسة المصرفية المصدرة: .....

الفرع: .....

كفالة رقم: .....

السادة/ شركة الكهرباء الوطنية م.ع

بناءً على طلب السادة (اسم المتعهد–عنوانه) نتعهد نحن (البنك المحلي) بشكل غير قابل للنقض وبدون أي شرط أن ندفع لكم أو لممثليكم القانونيين لدى أول طلب خطي منكم ورغم أي معارضة من المكفول ودون الحاجة إلى توجيه إخطار عدلي أو اتخاذ أي إجراء قضائي مبلغ) بالأرقام (..... (المبلغ بالكلمات) ..... وذلك ضماناً لحسن تنفيذ العطاء رقم (2026/20)

وتبقى هذه الكفالة سارية المفعول من تاريخ صدورها ولغاية / / ثم تمدد تلقائياً لثلاثة أشهر ثم تمدد لفترات متعاقبة ولا تُلغى هذه الكفالة إلا بكتاب رسمي صادر وموقع من قبلكم.

وتفضلوا بقبول فائق الاحترام ،،،

البنك المحلي.....

عطاء رقم (2026/20)

كفالــة صيانـــة

السادة/ شركة الكهرباء الوطنية م.ع

البنك او المؤسسة المصرفية المُصدرة:.....

الفرع : .....

كفالة الصيانة رقم: .....

بناءً على طلب السادة (اسم المتعهد–عنوانه) نتعهد نحن (البنك المحلي) بشكل غير قابل للنقض وبدون أي شرط أن ندفع لكم أو لممثليكم القانونيين لدى أول طلب خطي منكم ورغم أي معارضة من المكفول ودون الحاجة إلى توجيه إخطار عدلي أو اتخاذ أي إجراء قضائي

مبلغ (بالأرقام) ..... (المبلغ بالكلمات) ..... وذلك ضمان صيانة للعطاء رقم..... .

وتبقى هذه الكفالة سارية المفعول من تاريخ صدورها ولغاية / / ثم تمدد تلقائياً لثلاثة أشهر ثم تمدد لفترات متعاقبة ولا تُلغى هذه الكفالة إلا بكتاب رسمي صادر وموقع من قبلكم.

وتفضلوا بقبول فائق الاحترام،

البنك المحلي

تعليمات عامة للمشتركين

==========

1- تسلم العروض إلكترونياً عبر منصة الشراء الموحد JONEPS

(الموقع الإلكتروني : www.joneps.gov.jo)

2- على جميع المشاركين تقديم ما يثبت حصولهم على وثائـق العطاء (سند القبض) بموجب احكام النظام قبل ايداع العروض.

3- يجوز للمناقصين تقديم طلبات إيضاح على وثيقة الشراء من خلال (الموقع الإلكتروني : www.joneps.gov.jo).

4- لا يجوز للمناقص ان يقدم اكثر من عرض لنفس العطاء فيما يخص استدراجات الاشغال والخدمات الفنية و/او لنفس المادة فيما يخص استدراجات اللوازم سواء كان منفردا او بائتلاف او بشراكة مع مناقص اخر.

5- لا تقبل العروض غير الموقعة حسب الأصول أو التي ترد متأخرة ولا ينظر في العروض الناقصة نقصاً معيباً.

6- على المناقص أن يرفق مع عرضه عنواناً ثابتاً يرسل عليه جميع المكاتبات المتعلقة بالعطاء وعليه ان يبلغ الشركة بكتاب مسجل عن أي تغيير او تعديل في عنوانه، وإلا فإنها لا تكون ملزمة بمراعاة هذا التغيير او التعديل وتعتبر جميع المكاتبات التي تترك له في المحل المذكور او ترسل بالبريد المسجل وكأنها وصلت فعلاً وسلمت في حينها.

7- يصرح المناقص ان عرضه لم يقدم بناءً على علاقة مع مناقص آخر.

8- للمناقص أو وكيلة المفوض حضور جلسة فتح العطاء لسماع قراءة أسعار العروض عند فتحها إذا كانت هنالك دعوة لذلك.

9- يحق للمناقص الذي يدعي أنه لحقت به خسارة أو أي ضرر نتيجة لقرار أو إجراء أو امتناع عن اتخاذ إجراء من الشركة أو يدعي أن لجان الشراء خالفت ما ورد في وثائق الشراء أو أحكام هذا النظام والتعليمات الصادرة بموجبه، أن يتقدم باعتراض في المرحلة الأولى وبشكوى في المرحلة الثانية وفقا لأحكام النظام.

10- يجوز للمناقصين تقديم طلبات اعتراض على الوثيقة أو أي قرار أو إجراء اتخذته الشركة أو لجنة الشراء يتعلق بإجراءات الشراء وفق أحكام النظام رقم(8) لسنة 2022 والتعليمات الصادرة بموجبه.

شروط عامة

==========

1- تشترط الشركة ويقبل المناقص ان يبقى العرض نافذ المفعول وغير جائز الرجوع عنه لمدة تسعون يوماً من التاريخ المحدد لقبول العروض الا اذا نصت وثيقة العطاء على خلاف ذلك.

2- على المناقص التدقيق في دعوة العطاء والشروط والتعليمات الملحقة بها وكذلك التدقيق في جدول الاسعاروتسعير كافة البنود وهو الذي يتحمل النتائج المترتبه على عدم قيامه بهذا التدقيق بصورة صحيحه.

3- تحتفظ الشركة لنفسها بحق استبعاد أي عرض لا يكون واضحاً بصوره كافية او يحمل أكثر من تفسير أو إذا كان ناقصاً في بيان مواصفات أي عمل من أعمال العطاء او شرط أو لم يقدم على النموذج المرفق بدعوة العطاء .

4- للشركة الحق في تسعير بعض البنود التي لم يتم تسعيرها من قبل المناقص وعلى أساس أقل سعر مقدم وذلك في حال تم الإحالة عليه وعلى المناقص الإلتزام بالسعر.

5- للشركة الحق في الغاء العطاء او اعادة طرحه حسب ماتراه ضرورياً للمصلحه العامه وبدون ابداء الاسباب، وفي هذه الحالة تعاد التأمينات الذين قاموا بتقديمها ولا تتحمل الشركة اية مسؤولية عن اية خسارة او ضرر يلحق بالمناقصين نتيجة هذا الإجراء و دون أن يكون لاي من المناقصين الحق في الرجوع على الشركة باي خسارة أو ضرر ولا يترتب على الشركة أي التزامات مادية أو غير مادية مقابل ذلك وتنشر قرارها على موقعها الالكتروني وعلى البوابة الالكترونية

6- الشركة غير ملزمة باحالة كافة الاعمال والخدمات المطلوبة وغير ملزمة بالاحالة اصلاً ولها ان تجزئ الاحالة حسبما تراه مناسباً .

7- يوافق المناقص على أن إصدار كتاب الإحالة من الشركة يشكل مع وثائق العطاء الأخرى عقداً ملزماً للطرفين (المناقص والشركة).

8- يحدد في عرض المناقص إسم المفوض بالتوقيع على عقد الشراء نيابة عنه في حال الاحالة عليه.

9- أن لا تكون للمناقص مصلحة متعارضة تؤثر في إبرام عقد الشراء.

10- أن لا يكون المناقص من المحرومين من الاشتراك في عمليات الشراء بموجب أحكام النظام.

11- في حال السماح لغير الاردني بالمشاركة يتعين عليه اثبات الامتثال بجميع متطلبات التأهيل الواردة في الوثيقة

12- للشركة ان تزيد أو تنقص من الاعمال أو الخدمات المطلوبة بناءً على حاجتها الطارئة في حدود 25% ودون ان يكون للمناقص الحق في زيادة الاسعار مهما كانت الأسباب .

13- للشركة الحق في ان ترفض كل او بعض العروض المقدمه اليها دون ان يكون لاي من المناقصين الحق في الرجوع عليها بأية خسارة او ضرر ناشئ عن تقديم عرضه، كما انها لا تلتزم بالإحالة على أرخص الاسعار.

14- يوافق المناقص على أن إصدار كتاب الإحالة من الشركة يشكل مع وثائق العطاء الأخرى عقداً ملزماً للطرفين (المناقص والشركة).

15- يحدد في عرض المناقص إسم المفوض بالتوقيع على عقد الشراء نيابة عنه في حال الاحالة عليه.

16- على المناقص عند الطلب تقديم بينات بخبرته ومقدرته ودرجة الخدمه المتوفره لديه والاهلية القانونية ومركزه المالي للدلاله له على قدرته على الوفاء بالتزامات ومتطلبات العطاء.

17- تحتفظ لجنة الشراء بحق تصحيح اخطاء الطباعة او الكتابة في العقود المبرمة مع المناقص الفائز.

18- لا يكون أي تعديل او تغيير في الشروط الوارده في العقد ملزماً لشركة الكهرباء الوطنية إلا إذا كان مكتوباً وموقعاً من لجنة الشراء.

19- على المناقص الذي تمت الاحالة عليه وقبل توقيع العقد دفع الرسوم المقررة بمقتضى أحكام التشريعات النافذة وتقديم تأمين حسن التنفيذ وفقا للتعليمات الصادرة بموجب أحكام هذا النظام وكما هو محدد في وثائق الشراء.

20- بعد احالة العطاء وتقديم الخدمات ، يجب على المتعهد الإلتزام بتنفيذ كافة الإلتزامات المترتبة عليه حسب القانون الاردني ومن ضمنها ضريبة الدخل والمبيعات ومتطلبات الضمان الإجتماعي و إحضار براءة ذمة سارية المفعول من دائرة ضريبة الدخل عند تقديم المطالبات الماليه ، ولن يتم تسديد الدفعات النهائيه واعادة كفالة حسن التنفيذ الا بعد ان يقوم المتعهد بإحضار براءة الذمه المطلوبه.

21- في حال قدم المناقص رسالة نوايا بدلا من اتفاقية إئتلاف مصدقة يجب تقديم اتفاقية الائتلاف مصدقة أصوليا قبل الإحالة النهائية

22- في حال توافر المعايير الفنية والمتطلبات الواردة في وثائق الشراء في العرض الأقل سعراً تتم الاحالة عليه على أساس الارخص المطابق.

23- يجوز للمناقص ان يرفق مع عرضه بعض البدائل الاختيارية اذا سمحت وثائق الشراء بذلك وعلى لجنة الشراء دراسة العرض او البديل المغطى بتأمين دخول العطاء واستبعاد العرض او البديل الغير مغطى بتأمين دخول العطاء

24- لا يجوز لمن احيل عليه العطاء ان يتنازل لاي شخص عن كل العقد او جزء منه بدون الحصول على اذن كتابي من الشركه واية مخالفه لهذا النص تخول الشركه حق الغاء العقد بدون انذار وبدون حاجة للالتجاء للقضاء ويتحمل المتنازل أية خسائر تنجم عن عملة هذا.

25- يبقى المحال عليه العطاء مسؤولاً بالتضامن مع المتنازل له تجاه الشركه عن تنفيذ العقد وفقاً للشروط في حالة موافقة الشركه على التنازل عن كل العقد او جزء منه.

26- على لجنة الشراء مصادرة تأمين دخول العطاء كليا او جزئيا في أي من الحالات التالية:-

- **اذا سحب المناقص العرض الذي قدمه أو عدله بعد انتهاء المدة الزمنية لتقديمه أواذا لم يلتزم به أو بجزء منه.**
- **اذا رفض المناقص الفائز قبول تصحيح خطأ حسابي ظهر في العرض.**
- **اذا لم يوقع المناقص على عقد الشراء خلال المدة المحددة في إشعار الإحالة النهائية أو اذا لم يقدم تأمين حسن التنفيذ إذا نصت وثائق الشراء على وجوب تقديمه.**
- **اذا قدم المناقص معلومات غير صحيحة أو غش في المعلومات أو الوثائق التي قدمها لغايات المشاركة في العطاء .**

27- إذا تخلف المناقص الذي احيل عليه العطاء عن تنفيذ التزاماته بموجب العقد او قصر في ذلك او تأخر في تقديم كفالة حسن التنفيذ أو قصر في إنجاز الأعمال المطلوبة فيجوز الغاء العقد المبرم معه وشراء الاعمال او الخدمات موضوع العقد من قبل أي مصدر اخر على حسابه ونفقاته.

28- للشركة الحق بأن ترفض أي عرض إذا اتضح لها أن المناقص مارس سلوكاً أو تصرفاً من التصرفات المخالفة لأحكام النظام (8) لعام 2022 ويتم إبلاغ المناقص المعني بقرارها مع إتخاذ الإجراءات اللازمة بحقه.

29- تعتبر الشروط والمواصفات الواردة في الوثيقة والعرض وكتب الالتزام المقدمين من المناقص جزءا لا يتجزأ من العقد الا اذا ورد خلاف ذلك بقرار الاحالة.

30- اذا وجد تعارض في وثائق الشراء بين الشروط العامة والشروط الخاصة فيؤخذ بما ورد بالشروط الخاصة

31- يلتزم المتعهد بالرسوم المفروضه وفقاً لاحكام القوانين والانظمه المعمول بها في المملكة الأردنية الهاشمية.

32- يطلب من المتعهدين بيان الرقم الوطني الضريبي.

33- يطلب من المتعهدين تقديم رخصة مزاولة مهنة مصدقة وسارية المفعول حسب الأصول.

34- تخضع هذه الوثيقة لأحكام وتعليمات نظام المشتريات الحكومي رقم (8) لسنة 2022.

الأسعار

==========

1- سيكون السعر الأقل والقدرة على تلبية المتطلبات المطلوبة في مواصفات العطاء هي المعايير في إختيار المناقص الذي سيتم الإحالة عليه.

2- يعتبر سعر عقد الشراء ثابتا

الدفـــــع

يكون دفع المستحقات المالية بناء على تقديم مطالبة مالية متضمنة أي معلومات تتطلبها شروط الدفع وبعد استلام المواد من قبل لجنة الاستلام وعمل مستندات الإدخال اللازمة.

Network Detection and Response (NDR)

Objectives

This document is an invitation for qualified bidders to offer the Network Detection and Response (NDR) system.

NEPCO intend to acquire Network Detection and Response (NDR) system to achieve deep visibility and continually monitor the network traffic in real-time to swiftly detect and respond to cyber threats.

To ensure the data sovereignty, the NDR system shall be installed as on-prem appliance in NEPCO headquarter. The system must empower the Security Operation Center (SOC) of NEPCO with sophisticated tools for detection anomalies, conducting threat hunting and executing rapid incident response and digital forensics.

Bidders Eligibility

- Vendors who have been recognized in the Gartner Magic Quadrant for NDR or The Forrester Wave for Network Analysis and Visibility (NAV) at least for the 2025 will be eligible for the tender evaluation. Bidders are required to provide official documentation or report excerpts as evidence.
- Bidders shall maintain a valid partnership for the offered NDR system, the partnership certificate must be submitted as part of the offer to verify the eligibility.
- Bidders must submit at least three (3) professional references for active projects of a similar scope and complexity. Each reference must include contact details and a brief project overview. To demonstrate local market proficiency, at least two (2) of these projects must be within local organizations.

Evaluation Criteria

- Bidder eligibility
- Compliance with technical specification
- Training
- Financial Offer

Scope of work

- Procurement and delivery of full NDR system
- Installation of NDR system in NEPCO headquarter
- Configuration and integration of NDR system with other systems
- Training of NEPCO personnel

Technical Specifications

The NDR system will be deployed in the main data center in order to provide deep visibility into core network traffic, empowering the cybersecurity team to detect, mitigate, and defend against evolving threats. As well, to ensure the cybersecurity team can identify and remediate threats effectively while hardening system defenses.

The following specifications shall be met in the offered platform.

NDR Appliance

- Necessary hardware must be enterprise-grade class and adhere to a standard 19-inch rack mountable form factor
- The NDR system must be secure and hardened operating system
- Available capture (mirroring) interfaces: Two MMF 10Gbps and two copper 1Gbps
- Management interfaces: One Copper 1Gbps out of band (OOB) management
- Support expansion modules for additional interfaces for traffic mirroring
- It shall be capable to store metadata records for incidents and network connections at least for 60 days lookback
- Dual 100/240AC power supplies

Throughput

- Average traffic throughput: 1.6 Gbps
- The platform shall be expandable to allow traffic up to 3 Gbps
- The input traffic can be through port mirroring (SPAN)
- Optional: input traffic can be also captured through network TAP or packet broker.

Detection and Response

- The NDR solution must be capable of proactive threat detection utilizing a multi-layered approach to identify both known and zero-day threats like cyber threat intelligence, behavioral anomaly detection, and advanced AI/Machine Learning models
- It is capable to detect zero-day attacks
- Perform real-time threat detection and mapped it to MITRE ATT@CK
- A dedicated page/window/box shall exist to display the incident details, it shall contain enormous remarkable details related to the incident
- Extensive descriptions, references, and documentation for detected incidents.
- The incident details shall include all relevant information that are needed for incident response which shall include but not be limited to malicious file name, malicious file hash value, malicious URL, attacker IP, GeoIP

- Native On-prem threat detection and response, the platform shall actively keep working without the needs for connection with vendor infrastructure
- Detected incidents are classified through threat type/category
- The detection details shall include threat type like Ransomware attack, DDoS attack, Reconnaissance attack, etc.
- Risk scoring for detected threats
- Can add comment when handling an incident
- It is able to send alerts for detected incidents through email and SMS, these alerts can be defined in the platform
- The platform shall provide capabilities for automatic and manual response
- Automatic response is achieved though integration with cybersecurity solutions like EDR, firewalls and others for taking actions to contain the active threats
- Capable to analyze or decrypt the encrypted traffic to provide high-fidelity visibility of various protocols like HTTPS, Kerberos, SMB, LDAP
- Analyze network protocols and extract and display granular protocol metadata, **including but not limited to**:
  DNS attributes (record types, response codes) and HTTP transaction details (URLs, status codes, and methods), Kerberos attributes (Group members, response Type, Error Type), LDAP attributes (Distinguished Names, Error Codes, Message Types), RPC attributes
- The platform provides comprehensive visibility into user activities
- Facilitate incident investigation through pivoting from incident page to launch lookup in VirusTotal by clicking on an Indicator of Compromise (IOC)

Devices Inventory

- The system shall be architected to support a minimum of 3,000 concurrent devices
- It shall be highly scalable to accommodate a 200% increase in managed devices, ensuring consistency without degradation in system performance
- Automatic assets discovery and classification
- Automatic and manual assets updates
- Device tagging
- Discovered Asset Information: First seen, Last seen, IP address. MAC address, hostname, operating system, protocols used

Integration

- Capable to integrate with different protection platforms which include but not be limited to EDR, firewalls, email security

- Capable to integrate with cybersecurity monitoring and automation solutions like SIEM, SOAR
- Capable to integrate with threat intelligence feeds and TID solutions
- Capable to integrate with email and SMS platforms to send alter messages
- Capable to integrate with corporate active directory and LDAP

Search and Filter facilities:

- Able to search for incident using incident ID, threat type and other criteria
- Able to search for assets
- Able to search for incident during defined time interval
- Able to filter various facilities based on different key words

Reports and Dashboards

- The platform capable to generate reports in different format (pdf, xlsx, csv,…)
- The generated report shall be customized by adding and removing particular fields
- Reports can be generated for particular incidents includes all related information
- The dashboards shall be customized
- The dashboards can display network traffic throughput for total traffic, top N of: used protocol, sources, destinations, requested domains, Files transferred, HTTP status code, etc
- Various prebuilt dashboards like number of users/activities/TLS sessions, list of TLS certificates, DNS Requested Domains, AD User Account Error Statistics, Invalid Passwords Statistics
- Executive summary dashboard and reports

System Status

- Various dashboards and reports to monitor the system health
- Number of discovered devices
- Network throughput
- CPU usage and Storage usage
- Packet/Byte rate
- Metadata records count and rate
- Log rate

Platform Management

- The system shall be accessed and managed through web browsers, SSH and API
- It shall facilitate multi-user environments with customizable permission levels
- It shall support concurrent multi-user access
- It shall support MFA when accessing the system, it shall be capable to work different MFA platforms
- Web access session timeout shall be defined by platform users

Warranty and Subscriptions

Warranty period support for the provide systems shall be for minimum three years after material received by NEPCO and putting it in operation.

The NDR system's components and modules shall be regularly updated to ensure optimal performance and continuous protection against evolving cyber threats. These updates are dependent on the specific NDR features in use, like Cyber Threat Intelligence (CTI), Artificial Intelligence (AI), Machine Learning (ML), and signature-based detection.

Any required annual licenses and software updates and upgrades shall be offered in two options:

- 1-year license bundle
- 3-year license bundle

These options should encompass software support, updates, upgrades, bug fixes, security feature updates and other related services.

Any additional license that is needed to provide the following capabilities shall be provided and clearly mentioned.

Training

The bidders will provide specialized, high-impact training to NEPCO cybersecurity team to ensure they possess the advanced technical competencies required for their roles. The mandated training is organized into two distinct segments; **NDR training** and **Microsoft Windows Server Infrastructure training**. Table below shows the number of participants:

No.	Training	Participants
1	NDR	4 Persons
2	Microsoft Windows Server Infrastructure	6 Persons

Official NDR Training

The bidders shall be responsible for the provision of official vendor training to the NEPCO staff to enable them to operate, maintain and troubleshoot the provided NDR system under this project. The training course(s) shall ensure that the NEPCO personnel are fully trained in handling detected cyber threats and fully capable to operate the system.

The training course shall cover the different skills that are needed to manage and operate the provided system and to have the full capability to deal with detected cyber incidents.

In Addition, the training curriculum shall encompass on how to interpret and tune "normal" network behaviour baselines to distinguish legitimate activity from sophisticated threats. Also, it shall encompass advanced diagnostic procedures and complex troubleshooting methodologies for the system

The course(s) shall be of sufficient length and pace and include sufficient practice exercises to ensure that the subject matter is covered thoroughly, and the trainees are able to demonstrate their understanding of what they have been taught.

The Bidders shall include in their offer an outline proposal in terms of content and duration for the training at the bidder/vendor premises. The training shall be arranged at training facility of the vendor or accredited by the vendor of the provided NDR.

Training shall be hands-on and conducted by experienced and certified instructor(s) who are familiar with the systems supplied. Each course attendee shall be provided with a full set of relevant course materials for each training course. All relevant equipment documentation shall be available during the training courses.

All costs associated with the training program shall be the responsibility of the bidders and shall be included in the bidder price.

Microsoft Windows Server Infrastructure Training

The objective of this course is to strengthen the capabilities of NEPCO cybersecurity team with a particular emphasis on Microsoft Windows Servers and their associated services. The training will provide the essential skills required to effectively understand and oversee the Windows Server environment.

The intended course shall include, **but not limited to** Domain Controller (DC), Active Directory (AD), DHCP, DNS, Hyper-V, manage security in AD, PowerShell, on-premises and hybrid networking infrastructure, IP Address Management (IPAM), Web Application Proxy, Encryption and Secure Windows Server.

The course(s) shall be of sufficient length and pace and include sufficient practice exercises to ensure that the subject matter is covered thoroughly, and the trainees are able to demonstrate their understanding of what they have been taught.

Training shall be hands-on and conducted by experienced and certified instructor(s) who are familiar with the systems supplied. All relevant equipment documentation shall be available during the training courses.

The Bidders shall include in their offer an outline proposal in terms of content and duration for training.

All costs associated with the additional training program shall be the responsibility of the bidders and shall be included in the bidder price.

Technical Compliance

The bidders are required to complete the following schedule in order to confirm the technical compliance, any deviation shall be mentioned by the bidders in this shedule.

No.	Technical Requirements	Compliance (Yes/No)	Comments
NDR Appliance			
1	Necessary hardware must be enterprise-grade class and adhere to a standard 19-inch rack mountable form factor		
2	The NDR system must be secure and hardened operating system		
3	Available capture (mirroring) interfaces: Two MMF 10Gbps and two copper 1Gbps		
4	Management interfaces: One Copper 1Gbps out of band (OOB) management		
5	Support expansion modules for additional interfaces for traffic mirroring		
6	Dual 100/240AC power supplies		
7	It shall be capable to store metadata records for incidents and network connections at least for 60 days lookback		
8	The NDR system shall be capable of performing or facilitating packet capture (PCAP) and storage through native capability or through seamless integration with external packet capture solutions		
Throughput			
9	Average traffic throughput: 2 Gbps		
10	The platform shall be expandable to allow traffic up to 4 Gbps		
11	The input traffic can be through port mirroring (SPAN)		
12	Optional: input traffic can be also captured through network TAP or packet broker		
Detection and Response			
13	The NDR solution must be capable of proactive threat detection utilizing a multi-layered approach. This shall include, but is not limited to, integrated threat intelligence, behavioral anomaly detection, and advanced AI/Machine Learning models to identify both known and zero-day threats		

14	It is capable to detect zero-day attacks		
15	Perform real-time threat detection and mapped it to MITRE ATT@CK		
16	A dedicated page/window/box shall exist to display the incident details, it shall contain enormous remarkable details related to the incident		
17	Extensive descriptions, references, and documentation for detected incidents.		
18	The incident details shall include all information needed for incident response which shall include but not be limited to malicious file name, malicious file hash value, malicious URL, attacker IP, GeoIP		
19	Native On-prem threat detection and response, the platform shall actively keep working without the needs for connection with vendor infrastructure		
20	Detected incidents are classified through threat type/category		
21	The detection details shall include threat type like Ransomware attack, DDoS attack, Reconnaissance attack, etc.		
22	Risk scoring for detected threats		
23	Can add comment when handling an incident		
24	It is able to send alerts for detected incidents through email and SMS, these alerts can be defined in the platform		
25	The platform shall provide capabilities for automatic and manual response		
26	Automatic response is achieved though integration with cybersecurity solutions like EDR, firewalls and others for taking actions to contain the active threats		
27	Capable to analyze or decrypt the encrypted traffic to provide high-fidelity visibility of various protocols like HTTPS, Kerberos, SMB, LDAP		
28	Analyze network protocols and extract and display granular protocol metadata, including **but not limited to**: DNS attributes (record types, response codes) and HTTP transaction details (URLs, status codes, and methods), Kerberos attributes (Group members, response Type, Error Type), LDAP attributes (Distinguished Names, Error Codes, Message Types), RPC attributes		

29	The platform provides comprehensive visibility into user activities		
30	Facilitate incident investigation through pivoting from incident page to launch lookup in VirusTotal by clicking on an Indicator of Compromise (IOC)		
Devices Inventory			
31	The system shall be architected to support a minimum of 3,000 concurrent devices		
32	It shall be highly scalable to accommodate a 300% increase in managed devices, ensuring consistency without degradation in system performance		
33	Automatic assets discovery and classification		
34	Automatic and manual assets updates		
35	Device tagging		
36	Discovered Asset Information: First seen, Last seen, IP address. MAC address, hostname, operating system, protocols used		
Integration			
37	Capable to integrate with different protection platforms which include but not be limited to EDR, firewalls, email security		
38	Capable to integrate with cybersecurity monitoring and automation solutions like SIEM, SOAR		
39	Capable to integrate with threat intelligence feeds and TID solutions		
40	Capable to integrate with email and SMS platforms to send alter messages		
41	Capable to integrate with corporate active directory and LDAP		
Search and Filter facilities			
42	Able to search for incident using incident ID, threat type and other criteria		
43	Able to search for assets		
44	Able to search for incident during defined time interval		
45	Able to filter various facilities based on different key words		

Reports and Dashboards			
46	The platform capable to generate reports in different format (pdf, xlsx, csv,…)		
47	The generated report shall be customized by adding and removing particular fields		
48	Reports can be generated for particular incidents includes all related information		
49	The dashboards shall be customized		
50	The dashboards can display network traffic throughput for total traffic, top N of: used protocol, sources, destinations, requested domains, Files transferred, HTTP status code, etc		
51	Various prebuilt dashboards like number of users/activities/TLS sessions, list of TLS certificates, DNS Requested Domains, AD User Account Error Statistics, Invalid Passwords Statistics		
52	Executive summary dashboard and reports		
System Status			
53	Various dashboards and reports to monitor the system health		
54	Number of discovered devices		
55	Network throughput		
56	CPU usage and Storage usage		
57	Packet/Byte rate		
58	Metadata records count and rate		
59	Log rate		
Platform Management			
60	The system shall be accessed and managed through web browsers, SSH and API		
61	It shall facilitate multi-user environments with customizable permission levels		
62	It shall support concurrent multi-user access		
63	It shall support MFA when accessing the system, it shall be capable to work different MFA platforms		
64	Web access session timeout shall be defined by platform users		

Payment Terms

- **First payment**: representing forty percent (40%) of the total contract value shall be remitted after the receipt of all hardware and materials at NEPCO stores.
- **Second payment**: representing thirty percent (30%) of the total contract value shall be remitted following the completion of successful installation, configuration and integration phases of delivered system.
- **Third payment**: representing twenty percent (25%) of the total contract value shall be remitted following the successful completion of all training courses
- **Final payment**: representing ten percent (5%) of the total contract value shall be remitted following the formal expiration following the formal expiration of the warranty period.