Poznań, 8 października 2024 r.

ZATWIERDZAM:

WIELKOPOLSKI KOMENDANT WOJEWÓDZKI
Państwowej Straży Pożarnej

st. bryg. mgr inż. Jacek Strużyński

ZAPROSZENIE DO ZŁOŻENIA OFERTY

(zwane dalej „Zaproszeniem")

ZAMAWIAJĄCY:
Komenda Wojewódzka Państwowej Straży Pożarnej w Poznaniu

zaprasza do złożenia oferty w postępowaniu o udzielenie zamówienia publicznego na:
„Zakup licencji oprogramowania antywirusowego
ESET PROTECT ADVANCED 1000 stanowisk na okres 2 lat"

Numer sprawy: WL.2370.32.2024

NACZELNIK WYDZIAŁU
INFORMATYKI I ŁĄCZNOŚCI
st. bryg. mgr inż. Grzegorz Lewicz

ZASTĘPCA NACZELNIKA
WYDZIAŁU LOGISTYKI
mł. bryg. mgr inż. Piotr Matysiak

I. INFORMACJE O ZAMAWIAJĄCYM

Komenda Wojewódzka Państwowej Straży Pożarnej w Poznaniu ul. Masztalarska 3, 61-767 Poznań.
REGON: 000684493 | NIP: 7781209832 | e-mail: kancelria@psp.wlkp.pl

II. PROCEDURA

Przedmiotowe postępowanie (rozeznanie cenowe) prowadzone jest przy użyciu środków komunikacji elektronicznej. Składanie ofert następuje za pośrednictwem platformy zakupowej (platformazakupowa.pl) dostępnej pod adresem internetowym: **https://platformazakupowa.pl/pn/wielkopolska_straz**, zwanej dalej „Platformą".

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup licencji oprogramowania antywirusowego ESET PROTECT ADVANCED 1000 stanowisk na okres 2 lat.
2. Zamawiający wymaga minimum 24 miesięcy gwarancji producenta na przedmiot zamówienia.
3. Wymagany dostęp w języku polskim do internetowego archiwum producenta dostępnego na stronie WWW.
4. Szczegółowy opis przedmiotu zamówienia zawiera załączniki nr 3 do Zaproszenia.
5. Państwa firma poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
6. Zamawiający Zastrzega, że postępowanie może zakończyć się brakiem wyboru oferty w przypadku niewystarczających środków na realizację zamówienia.
7. Szczegółowe warunki i sposób realizacji zamówienia określono w projekcie umowy, który stanowi załącznik nr 2 do Zaproszenia.

IV. TERMIN WYKONANIA ZAMÓWIENIA

Termin realizacji zamówienia: **30 dni od dnia podpisania umowy.**

V. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca będzie związany ofertą od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert, przez okres **30 dni.**

VI. TERMIN ZŁOŻENIA OFERTY ORAZ SPOSÓB KOMUNIKACJI

1. Postępowanie prowadzone jest w języku polskim w formie elektronicznej. Ofertę Wykonawca przekazuje do Zamawiającego wyłącznie za pośrednictwem Platformy. Link do postępowania znajduje się pod adresem:

   https://platformazakupowa.pl/pn/wielkopolska_straz/proceedings

2. Ofertę wraz z wymaganymi dokumentami (jeżeli dotyczy) należy złożyć (przekazać) do dnia:

   11 października 2024 r. do godziny 10:00.

3. Wszelkie informacje pomiędzy Zamawiającym a Wykonawcami będą przekazywane wyłącznie elektronicznie, za pośrednictwem Platformy w sekcji „Komunikaty".
4. Zamawiający informuje, że instrukcje korzystania z Platformy dotyczące w szczególności logowania, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.

VII. KRYTERIA WYBORU OFERTY ORAZ SPOSÓB OCENY

1. Za ofertę najkorzystniejszą w zostanie uznana oferta zawierająca najkorzystniejszy bilans punktów w kryteriach:
   a) Cena ofertowa – 100 %
2. Punkty powyższym kryteriom Zamawiający przyzna na podstawie:
   a) Cena ofertowa – C_{oferty} [100,00 pkt]
   W zakresie kryterium „cena ofertowa" oferta może uzyskać określoną ilość punktów wyliczoną na podstawie wzoru matematycznego. Cena ofertowa: matematyczne porównanie ceny oferty z najniższą ceną do ceny oferty badanej (cena najniższa otrzymuje łącznie 100,00 pkt). Wyliczenie wg wzoru:

$$C_{oferty} = \frac{\text{CENA OFERTY ZAWIERAJĄCEJ NAJNIŻSZĄ CENĘ}}{\text{CENA OFERTY BADANEJ}} \times 100{,}00 \text{ pkt}$$

   gdzie;
   cena oferty – cena brutto w PLN za dostawę przedmiotu zamówienia.

3. Punktacja przyznawana ofertom w poszczególnych kryteriach oceny ofert będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
4. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny, zamawiający wezwie wykonawców w wyznaczonym terminie do złożenia ofert dodatkowych.

VIII. OPIS SPOSOBU PRZYGOTOWANIA OFERT ORAZ WYMAGANIA ZAMAWIAJĄCEGO

1. Oferta musi być sporządzona w języku polskim. Zamawiający zaleca przygotowanie oferty w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub opatrzonej podpisem zaufanym lub podpisem osobistym(e-dowodem) przez osobę/osoby fizyczne (Wykonawca) lub jej pełnomocnika/ów lub osoby uprawnione do reprezentacji osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej.
2. Oferta powinna zawierać:
   a) podpisany załącznik nr 1 do Zaproszenia „Oferta cenowa",
   b) kopię pełnomocnictwa o ile ofertę podpisuje pełnomocnik.

IX. INFORMACJE DODATKOWE DOTYCZĄCE POSTĘPOWANIA

1. W celu zapewnienia porównywalności wszystkich ofert Zamawiający zastrzega sobie prawo do skontaktowania się z właściwymi Wykonawcami w celu uzupełnienia lub doprecyzowania oferty.
2. Zamawiający zastrzega sobie możliwość negocjacji warunków i ceny zamówienia oraz do rezygnacji z zamówienia bez podania przyczyny.
3. Niniejsze zaproszenie nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych oraz nie stanowi źródła zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert.
4. Zamawiający zastrzega, że całościowa oferowana cena stanowi informację publiczną w rozumieniu ustawy o dostępie do informacji publicznej i w przypadku zastrzeżenia jej przez Wykonawcę jako tajemnicy przedsiębiorstwa lub tajemnicy przedsiębiorcy oferta nie będzie rozpatrywana.

X. OCHRONA DANYCH OSOBOWYCH

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z dnia 4 maja 2016 r., str. 1; zwanym dalej "RODO") informujemy, że:
   1) administratorem Pani/Pana danych osobowych jest Wielkopolski Komendant Wojewódzki Państwowej Straży Pożarnej (61-767 Poznań ul. Masztalarska 3, tel.: 47 77 16 000, fax: 61 22 20 500, e-mail: kancelaria@psp.wlkp.pl);
   2) administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: http://www.psp.wlkp.pl/iod/;
   3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego;
   4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania;
   5) Pani/Pana dane osobowe będą przechowywane, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
   6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego;
   7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
   8) posiada Pani/Pan:
      a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);

b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy*);
c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*);
d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) nie przysługuje Pani/Panu:
a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;
10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

XI. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 - Oferta cenowa.
Załącznik nr 2 - Projekt umowy.
Załącznik nr 3 - Opis przedmiotu zamówienia.

OFERTA CENOWA

ZAMAWIAJĄCY:
Komenda Wojewódzka Państwowej Straży Pożarnej w Poznaniu
ADRES: ul. Masztalarska 3
KOD: 61-767 **MIASTO:** Poznań
TELEFON: +48 47 77 16 000 | **FAX:** +48 61 22 20 566 | **E-MAIL:** kancelaria@psp.wlkp.pl
NIP: 7781209832 | **REGON:** 000684493

DANE WYKONAWCY:
Wykonawca 1: .....
ADRES: .....
KOD: ..... | **MIASTO:** ..... | **KRAJ:** .....
TELEFON: ..... | **FAX:** ..... | **E-MAIL:** .....@.....
NIP: ..... | **REGON:** ..... | **KRS:** .....

Wykonawca 1 jest:
1) mikroprzedsiębiorstwem TAK / NIE*
2) małym przedsiębiorstwem TAK / NIE*
3) średnim przedsiębiorstwem TAK / NIE*
(* niepotrzebne skreślić)

Wykonawca[1] 2: .....
ADRES: .....
KOD: ..... | **MIASTO:** ..... | **KRAJ:** .....
TELEFON: ..... | **FAX:** ..... | **E-MAIL:** .....@.....
NIP: ..... | **REGON:** ..... | **KRS:** .....

Wykonawca 2 jest:
1) mikroprzedsiębiorstwem TAK / NIE*
2) małym przedsiębiorstwem TAK / NIE*
3) średnim przedsiębiorstwem TAK / NIE*
(* niepotrzebne skreślić)

Pełnomocnik[1] do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia **(np. lider konsorcjum):** .....
ADRES: .....
KOD: ..... | **MIASTO:** ..... | **KRAJ:** .....
TELEFON: ..... | **FAX:** ..... | **E-MAIL:** .....@.....
NIP: ..... | **REGON:** ..... | **KRS:** .....

Pełnomocnik jest:
1) mikroprzedsiębiorstwem TAK / NIE*
2) małym przedsiębiorstwem TAK / NIE*
3) średnim przedsiębiorstwem TAK / NIE*
(* niepotrzebne skreślić)

[1] wypełniają jedynie Wykonawcy wspólne ubiegający się o udzielenie zamówienia (np. konsorcja).

Jako Wykonawca w postępowaniu prowadzonym w trybie rozeznania cenowego na:

„Zakup licencji oprogramowania antywirusowego

ESET PROTECT ADVANCED 1000 stanowisk na okres 2 lat"

1. Oferuje/my/ wykonanie przedmiotu zamówienia tj. Zakup licencji oprogramowania antywirusowego ESET PROTECT ADVANCED 1000 stanowisk na okres 2 lat w rzeczowym zakresie wyszczególnionym poniżej:

I	Nazwa	Ilość sztuk	Element składowy dostawy
I.1	Oprogramowanie antywirusowe ESET PROTECT ADVANCED	1000 (licencji)	System musi zapewniać między innymi * : 1. Administracja zdalna w chmurze. 2. Ochrona stacji roboczych. 3. Ochrona serwera. 4. Szyfrowanie. 5. Ochrona urządzeń mobilnych opartych o system Android. 6. Sandbox w chmurze.
II	**Gwarancja:**		
II.1	Zamawiający wymaga na przedmiot zamówienia minimum: 24 miesięcy gwarancji producenta.		(wpisać długość okresu gwarancji w miesiącach)

2. **Informujemy, że wybór naszej oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego:

.....

należy podać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego wskazując ich wartość bez kwoty podatku (wartość netto) oraz wskazać stawkę podatku VAT, która będzie miała zastosowanie.

** jeżeli na Wykonawcy spoczywa obowiązek podatkowy związany z realizacją zamówienia, przed podpisaniem druku „Oferta cenowa" należy zapis wykreślić lub wpisać nie dotyczy.

3. Oświadczam/y/, że cena brutto zawiera wszystkie koszty związane z wykonaniem przedmiotu zamówienia oraz, że do wyliczenia poszczególnych cen i wartości brutto, zastosowaliśmy właściwą stawkę podatku od towarów i usług (VAT) w wysokości procentowej obowiązującej w dniu wszczęcia postępowania.

4. Warunki płatności: faktura płatna przelewam w terminie **30 dni**.

5. Okres realizacji zamówienia: **30 dni od dnia podpisania umowy**

6. Oświadczam/y/, że zapoznaliśmy się ze treścią Zaproszenia i nie wnosimy do niego zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty.

7. Zobowiązuje/my/ się do dostarczenia przedmiotu zamówienia zgodnego z naszą ofertą i opisem przedmiotu zamówienia, na warunkach określonych przez Zamawiającego.

8. Oświadczam/y/, że zapoznałem(-liśmy) się z załączonymi do Zaproszenia projektem umowy (Załącznik nr 2 do Zaproszenia) i zobowiązuję(-emy) się - w przypadku uznania mojej (naszej) oferty za najkorzystniejszą - do zawarcia umowy na ustalonych tam warunkach, w miejscu i terminie wyznaczonym przez zamawiającego.

9. Oświadczam/y/, że czujemy się związani niniejszą ofertą przez okres **30 dni**.

10. Oświadczam/y/, że nie zachodzą w stosunku do mnie/nas przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego

(Dz. U. 2022 poz. 835 z późn. zm.)[1].

13. **Zamówienie zrealizujemy** sami * / przy udziale podwykonawców * **(* niepotrzebne skreślić)**, którzy będą wykonywać następujące prace wchodzące w zakres przedmiotu zamówienia:
1) .....
(zakres i/lub udział procentowy i/lub wartość prac, które będzie wykonywać podwykonawca)

.....

Dokument należy wypełnić i podpisać.
Zamawiający zaleca użycie podpisu kwalifikowanego lub podpisu zaufanego lub podpisu osobistego. Zamawiający zaleca zapisanie dokumentu w formacie PDF.

[1] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą"*, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

UMOWA
NUMER WO.0270.___.2024

zawarta w dniu _____ 2024 roku w Poznaniu pomiędzy:

firmą:

.....

reprezentowaną przez:

.....

zwaną dalej **WYKONAWCĄ**

a

Skarbem Państwa reprezentowanym przez Wielkopolskiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej st. bryg. Jacka STRUŻYŃSKIEGO
przy kontrasygnacie p. o. Głównego Księgowego bryg. Aleksandry Fojt
adres do korespondencji:
Komenda Wojewódzka Państwowej Straży Pożarnej
61-767 Poznań, ul. Masztalarska 3
zwanym dalej **ZAMAWIAJĄCYM**

§ 1.
PRZEDMIOT UMOWY

1. WYKONAWCA zobowiązuje się dostarczyć dla Komendy Wojewódzkiej PSP w Poznaniu **licencję oprogramowania antywirusowego ESET PROTECT ADVANCED na 1000 stanowisk komputerowych, na okres 2 lat** – zgodnie ze złożoną ofertą, która stanowi jednocześnie załącznik nr 1 do niniejszej umowy.
2. ZAMAWIAJĄCY zobowiązuje się do odebrania przedmiotu umowy i zapłacenia WYKONAWCY należności.

§ 2.
CENA I WARUNKI PŁATNOŚCI

1. Cena brutto przedmiotu umowy wynosi: ..... PLN (słownie: ..... 00/100).
2. WYKONAWCA wystawi na ZAMAWIAJĄCEGO fakturę w języku polskim lub faktura będzie posiadać polską wersję językową, przy czym w przypadku wątpliwości co do treści faktury sporządzonej w języku innym niż polski, wiążąca dla ZAMAWIAJĄCEGO będzie treść polskiej wersji językowej.
3. Faktura może zostać wystawiona dopiero po wykonaniu weryfikacji poprawności działania przedmiotu zamówienia oraz poinformowaniu droga e-mail-ową o dokonanej weryfikacji i przygotowaniu protokołu odbioru.
4. ZAMAWIAJĄCY zapłaci WYKONAWCY należność za odebrany przedmiot umowy w ciągu 30 dni od daty otrzymania przez ZAMAWIAJĄCEGO faktury.
5. Termin płatności uważa się za zachowany, jeżeli obciążenie rachunku ZAMAWIAJĄCEGO nastąpi najpóźniej w ostatnim dniu płatności.
6. Strony zastrzegają, że przelew wierzytelności wynikających z niniejszej umowy nie może nastąpić bez zgody dłużnika wyrażonej na piśmie.
7. ZAMAWIAJĄCY informuje, że posiada skrzynkę PEPPOL na Platformie Elektronicznego Fakturowania umożliwiającą odbiór ustrukturyzowanych faktur elektronicznych. Numer identyfikatora konta: **7781209832**.

§ 3.
TERMIN REALIZACJI PRZEDMIOTU UMOWY

1. WYKONAWCA zobowiązuje się zrealizować przedmiot umowy w terminie 30 dni od dnia zawarcia niniejszej umowy, tj. do dnia: ..... 2024 r.
2. Termin realizacji umowy zostaje zachowany, jeżeli odbiór odbędzie się w terminie, o którym mowa powyżej.

§ 4.
ODBIÓR PRZEDMIOTU UMOWY

1. WYKONAWCA przekaże ZAMAWIAJĄCEMU drogą elektroniczną przedmiot umowy oraz wskaże drogę elektroniczną pobrania materiałów niezbędnych do prawidłowego działania przedmiotu umowy.

ZAMAWIAJĄCY przystąpi do odbioru w ciągu 3 dni od daty przekazania. Strony dopuszczają zawiadomienie w formie elektronicznej. Zawiadomienie należy kierować na adres: **WIL@PSP.WLKP.PL**

2. ZAMAWIAJĄCY dokona **zweryfikowania** prawidłowości i zgodności z zamówieniem w terminie 7 dni od otrzymania przedmiotu umowy zgodnie z pkt.1.
3. Formalny odbiór przedmiotu umowy odbędzie się poprzez protokół odbioru, który zostanie sporządzony w 2 egzemplarzach, po 1 egzemplarzu dla każdej ze stron i podpisany przez obie strony w ciągu 7 dni od stwierdzenia, że dostarczony produkt działa zgodnie z oczekiwaniami oraz jest zgodny z przedmiotem umowy.
4. W przypadku stwierdzenia, podczas odbioru bądź weryfikacji, usterek bądź niezgodności, WYKONAWCA zobowiązuje się do niezwłocznego ich usunięcia lub wymiany przedmiotu umowy na wolny od usterek.

§ 5.
DOKUMENTACJA TECHNICZNA

1. WYKONAWCA wskaże podczas odbioru elektroniczną drogę pobrania polskojęzycznej dokumentacji oraz instrukcji obsługi i konserwacji przedmiotu umowy.

§ 6.
GWARANCJA I NAPRAWA

1. WYKONAWCA udziela ZAMAWIAJĄCEMU ..... miesięcy gwarancji na przedmiot umowy.
2. Wszystkie dostarczone licencje muszą być objęte gwarancją producenta:
   - możliwość zgłaszania problemów przez 7 dni w tygodniu przez 24h na dobę telefonicznie lub/i drogą elektroniczną lub/i poprzez portal internetowy producenta,
   - zapewnienie elektronicznego dostępu do informacji w języku polskim lub angielskim na temat posiadanego oprogramowania, biuletynów technicznych, poprawek programistycznych,
   - zapewnienie dostępu do aktualizacji umożliwiających identyfikację najnowszych wirusów i szkodliwych programów w czasie trwania niniejszej umowy, bez limitu określającego częstotliwość pobierania i bez limitu liczby pobrań.
3. WYKONAWCA jest zobowiązany do wykonania świadczeń gwarancyjnych z należytą starannością zgodnie ze standardami obowiązującymi w branży informatycznej.

§ 7.
KARY UMOWNE

1. Jeżeli WYKONAWCA opóźni termin wydania przedmiotu umowy w stosunku do terminu uzgodnionego w umowie zapłaci ZAMAWIAJĄCEMU karę umowną w wysokości 0,2 % wartości brutto przedmiotu umowy za każdy dzień opóźnienia, nie więcej jednak niż 20 % ceny brutto przedmiotu umowy.
2. Jeżeli opóźnienie wydania przekroczy 14 dni ZAMAWIAJĄCY ma prawo odstąpić od umowy, jeżeli opóźnienie wystąpiło z winy WYKONAWCY. W takim przypadku ZAMAWIAJĄCY nie będzie zobowiązany zwrócić WYKONAWCY kosztów, jakie WYKONAWCA poniósł w związku z umową.
3. W przypadku odstąpienia od umowy z przyczyn leżących po stronie WYKONAWCY, ZAMAWIAJĄCY zapłaci WYKONAWCY karę umowną w wysokości 30% ceny brutto przedmiotu umowy.
4. Odstąpienie od umowy wymaga, pod rygorem nieważności, formy pisemnej poprzez złożenie oświadczenia drugiej stronie.
5. W przypadku, gdy WYKONAWCA nie dokona naprawy przedmiotu umowy w terminie wynikającym z protokołu naprawy gwarancyjnej zapłaci ZAMAWIAJĄCEMU karę umowną w wysokości 0,2 % wartości przedmiotu umowy za każdy dzień zwłoki.
6. W przypadku, gdy wysokość poniesionej szkody przewyższa wysokość kar zastrzeżonych w umowie ZAMAWIAJĄCY może żądać odszkodowania na zasadach ogólnych w wysokości odpowiadającej poniesionej szkodzie w pełnej wysokości.
7. Jeżeli ZAMAWIAJĄCY nie zapłaci należności za przedmiot umowy w terminie określonym w § 2 ust. 2 i 3 zapłaci WYKONAWCY ustawowe odsetki za opóźnienie w transakcjach handlowych za każdy dzień zwłoki.
8. WYKONAWCA wyraża zgodę na potrącenie kar umownych z należnego wynagrodzenia, z zastrzeżeniem ograniczeń wynikających z art. 15r ustawy z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020 r., poz. 1842, z późn. zm.).
9. Łączna maksymalna wysokość kar umownych, którą można obciążyć WYKONAWCĘ nie może przekroczyć 40% wynagrodzenia brutto.
10. Kara umowna staje się wymagalna z chwilą powstania podstawy do jej naliczenia.

§ 8.
ROZSTRZYGANIE SPORÓW I OBOWIĄZUJACE PRAWO

1. W przypadku powstania sporu na tle realizacji niniejszej umowy strony zawartej umowy zgodnie oświadczają, że poddają go rozstrzygnięciu przez sąd właściwy miejscowo dla ZAMAWIAJĄCEGO.
2. W sprawach nie objętych umową będą miały zastosowanie przepisy polskiego Kodeksu Cywilnego.

§ 9.
ZMIANA UMOWY

1. Zmiana postanowień niniejszej umowy może nastąpić wyłącznie za zgodą obu stron wyrażoną na piśmie pod rygorem nieważności.
2. ZAMAWIAJĄCY dopuszcza:
   a) aktualizację danych WYKONAWCY poprzez: zmianę nazwy firmy, zmianę adresu siedziby, zmianę formy prawnej itp.,
   b) zmianę wynagrodzenia brutto WYKONAWCY w przypadku ustawowej zmiany stawki podatku VAT (wyłącznie w zakresie tej stawki).

§ 10.
POSTANOWIENIA KOŃCOWE

1. Umowę sporządzono w 2 jednobrzmiących egzemplarzach w języku polskim, po 1 egzemplarzu dla ZAMAWIAJĄCEGO i dla WYKONAWCY.

ZA WYKONAWCĘ **ZA ZAMAWIAJĄCEGO**

Załączniki:

1) Załącznik nr 1 do umowy – kopia oferty cenowej Wykonawcy wraz z opisem przedmiotu zamówienia.

OPIS PRZEDMIOTU ZAMÓWIENIA

Minimalne wymagania techniczno – użytkowe

Nazwa	Ilość sztuk	Element składowy dostawy
Oprogramowanie antywirusowe ESET PROTECT ADVANCED	**1000 (licencji)**	System musi zapewniać między innymi * : 1. Administracja zdalna w chmurze, 2. Ochrona stacji roboczych, 3. Ochrona serwera, 4. Szyfrowanie, 5. Ochrona urządzeń mobilnych opartych o system Android, 6. Sandbox w chmurze. *) szczegółowy opis poszczególnych punktów systemu znajduje się poniżej.
Parametry techniczne dla wszystkich dostarczanych przenośnych jednostek komputerowych		
Min. 24 miesiące gwarancji podstawowej producenta. W czasie gwarancji usługa serwisu/helpdesku musi być świadczona przez autoryzowanego przedstawiciela producenta w języku polskim.		
Pozostałe		
Wymagany dostęp w języku polskim do internetowego archiwum producenta dostępnego na stronie WWW.		
Dostarczone oprogramowanie, w całości zamówienia, musi być najnowszą wersją w danym okresie zmówienia, musi pochodzić z oficjalnego kanału sprzedaży producenta na terenie Polski.		
Wykonawca dostarczy certyfikat oraz możliwość pobrania elektronicznej wersji objętej zamówieniem do siedziby zamawiającego, gdzie dokona on sprawdzenia kompletności zamówienia.		

*) SZCZEGÓŁOWY OPIS SKŁADNIKÓW SYSTEMU:

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami,

zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/ Windows11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody

heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    a. usunięcie zawartości urządzenia,
    b. przywrócenie urządzenie do ustawień fabrycznych,
    c. zablokowania urządzenia,
    d. uruchomienie sygnału dźwiękowego,
    e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
    a. nazwę aplikacji,
    b. nazwę pakietu,
    c. kategorię sklepu Google Play,
    d. uprawnienia aplikacji,
    e. pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.

12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. czysty,
    b. podejrzany,
    c. bardzo podejrzany,
    d. szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.