STAROSTWO POWIATOWE W LESZNIE

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego

prowadzonym w trybie podstawowym z możliwością negocjacji na:

zakup oprogramowania antywirusowego
wraz z oprogramowaniem do inwentaryzacji sprzętu w zakresie
udostępnienia prawa licencji użytkowania
dla Starostwa Powiatowego w Lesznie oraz jednostek organizacyjnych

Leszno, maj 2024 r.

I. Informacje o Zamawiającym

Starostwo Powiatowe w Lesznie
64-100 Leszno, Plac Kościuszki 4B
tel. 65 529-68-34, faks: 529-68-09
NIP: 697 19 52 864
Regon: 411102917
adres poczty elektronicznej: k.tyczynska@powiat-leszczynski.pl
adres strony internetowej: www.bip.powiat-leszczynski.pl

Adres strony internetowej prowadzonego postępowania:
https://platformazakupowa.pl/pn/powiat_leszczynski

Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia: **https://platformazakupowa.pl/pn/powiat_leszczynski**

Znak postępowania: OR.VI.272.3.2024
W korespondencji kierowanej do Zamawiającego należy posługiwać się tym znakiem.

II. Tryb udzielenia zamówienia

1. Postępowanie o udzielenie zamówienia prowadzone jest w **trybie podstawowym z możliwością przeprowadzenia negocjacji**, o którym mowa w art. 275 pkt 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2023 r., poz. 1605 ze zm.), zwanej dalej „ustawa Pzp" lub „Pzp".
2. Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3. W sprawach nieuregulowanych ustawą Pzp stosuje się przepisy ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny (Dz. U. z 2023 r., poz. 1610 ze zm.).

III. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest zakup oprogramowania antywirusowego wraz z oprogramowaniem do inwentaryzacji sprzętu w zakresie udostępnienia prawa licencji użytkowania, wdrożenie oraz przeszkolenie osób odpowiedzialnych za obsługę oprogramowania dla Starostwa Powiatowego w Lesznie oraz jednostek organizacyjnych.
   Ilość licencji: **180**.
   1) Starostwo Powiatowe w Lesznie – 121 licencji
   2) Powiatowe Centrum Pomocy Rodzinie w Lesznie – 10 licencji
   3) Zarząd Dróg Powiatowych – 12 licencji
   4) Specjalny Ośrodek Szkolno-Wychowawczy im. F. Ratajczaka – 20 licencji
   5) Zespół Szkół Specjalnych w Górznie – 2 licencje
   6) Powiatowa Poradnia Psychologiczno-Pedagogiczna – 11 licencji
   7) Środowiskowy Dom Samopomocy w Kąkolewie – 4 licencje.

   Okres udzielenia licencji: **24 miesiące** od dnia udzielenia licencji Zamawiającemu.
   Zakres zamówienia obejmuje wdrożenie oprogramowania w formie online lub stacjonarnie oraz przeszkolenie dwóch osób wskazanych przez Zamawiającego. Wymaga się przeprowadzenia dwóch szkoleń autoryzowanych przez producenta w trybie online lub stacjonarnie, zrealizowanych w ośrodku szkoleniowym producenta na terenie kraju. Po wdrożeniu oprogramowania Wykonawca zobowiązany jest zapewnić trzy konsultacje serwisowe zdalnie lub stacjonarnie.
2. Szczegółowy opis przedmiotu zamówienia zawarto w załączniku nr 1 do SWZ.

3. Oprogramowanie oferowane przez Wykonawcę musi wykonywać wszystkie funkcje podane przez Zamawiającego w opisie przedmiotu zamówienia.
4. Główny przedmiot zamówienia wg Wspólnego Słownika Zamówień (CPV): 48761000-0: pakiety oprogramowania antywirusowego, 72263000-6: usługi wdrażania oprogramowania.
5. Zamówienie realizowane jest w ramach konkursu grantowego pn.: „Cyberbezpieczny Samorząd", w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa".
6. Zamawiający nie przewiduje wymagań dotyczących zatrudnienia przez Wykonawcę lub Podwykonawcę na podstawie stosunku pracy, o których mowa w art. 95 ust. 1 Pzp ze względu na charakter i specyfikę usługi będącej przedmiotem zamówienia.

IV. Opis części zamówienia

1. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
2. Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania.

V. Termin wykonania zamówienia

Termin realizacji zamówienia: zgodnie z deklaracją wykonawcy złożoną na formularzu ofertowym, jednak nie dłuższy niż 12 dni kalendarzowych od dnia podpisania umowy. Termin wykonania zamówienia stanowi bowiem jedno z pozacenowych kryteriów wyboru oferty, które zostały opisane w rozdziale XV SWZ.

VI. Warunki udziału w postępowaniu oraz podstawy wykluczenia

1. Zamawiający nie określa warunków udziału w niniejszym postępowaniu zgodnie z art. 112 ust. 1 oraz w zw. z art. 57 pkt 2 ustawy Pzp.
2. **Informacja dla Wykonawców wspólnie ubiegających się o udzielenie zamówienia:**
   1) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo należy dołączyć do oferty.
   2) Wszelka korespondencja związana z postępowaniem o udzielenie zamówienia publicznego kierowana będzie do pełnomocnika wykonawców wspólnie ubiegających się o udzielenie zamówienia.
   3) W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenia o niepodleganiu wykluczeniu z postępowania składa każdy z Wykonawców.
   4) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni Wykonawcy (**załącznik nr 4 do SWZ**).
   5) Dokumenty wspólne takie jak: formularz ofertowy, oświadczenie dot. rodzajów dostaw wykonywanych przez poszczególne podmioty występujące wspólnie, składa pełnomocnik Wykonawców w imieniu wszystkich Wykonawców składających ofertę wspólną.

VII. Podstawy wykluczenia Wykonawcy z postępowania

1. Zgodnie z art. 108 ust. 1 Pzp z postępowania o udzielenie zamówienia wyklucza się Wykonawcę:
   1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,

c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. 2012 poz. 769 ze zm.),
g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1);
3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy Pzp, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

2. Zamawiający nie przewiduje fakultatywnych przesłanek wykluczenia, w oparciu o przepis art. 109 ust. 1 ustawy Pzp.
3. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy Pzp.
4. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
5. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2–5 i 7–10 ustawy Pzp, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:

1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
    a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
    b) zreorganizował personel,
    c) wdrożył system sprawozdawczości i kontroli,
    d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
    e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

6. Zamawiający ocenia, czy podjęte przez Wykonawcę czynności, o których mowa w ust. 5, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy. Jeżeli podjęte przez Wykonawcę czynności, o których mowa w ust. 5, nie są wystarczające do wykazania jego rzetelności, Zamawiający wyklucza Wykonawcę.
7. 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. z 2022 r., poz. 835), zwanej dalej „ustawą o przeciwdziałaniu wspierania agresji na Ukrainę", z postępowania o udzielenie zamówienia publicznego 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 o przeciwdziałaniu wspierania agresji na Ukrainę;
    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 o przeciwdziałaniu wspierania agresji na Ukrainę;
    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 o przeciwdziałaniu wspierania agresji na Ukrainę.
8. Wykluczenie następuje na okres trwania okoliczności określonych w ust. 7.

VIII. Informacja o przedmiotowych i podmiotowych środkach dowodowych

1. Wykonawca zobowiązany jest dołączyć do oferty **oświadczenie o niepodleganiu wykluczeniu** (oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp), w zakresie wskazanym przez Zamawiającego, którego wzór stanowi **załącznik nr 3** do SWZ.

2. Oświadczenie, o którym mowa w ust. 1 nie jest podmiotowym środkiem dowodowym. Stanowi dowód potwierdzający brak podstaw wykluczenia na dzień składania ofert.
3. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie, o którym mowa w ust. 1, składa każdy z Wykonawców odrębnie.
4. Zamawiający wymaga od Wykonawcy złożenia w oświadczeniu, o którym mowa w ust. 1 (**załącznik nr 3 do SWZ**), oświadczenia dotyczącego podwykonawcy niebędącego podmiotem udostępniającym zasoby, w zakresie podstaw wykluczenia, o których mowa w art.108 ust.1 oraz w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. w celu przeciwdziałania wspieraniu agresji Federacji Rosyjskiej na Ukrainę rozpoczętej w dniu 24 lutego 2022 r. (Dz.U. 15 z 2022 r. poz. 835).
5. **Oświadczenia, o których mowa powyżej należy złożyć, pod rygorem nieważności, w formie elektronicznej (tj. opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
6. Na podstawie art. 273 ust. 1 pkt 1 ustawy Pzp, Zamawiający nie wymaga złożenia w niniejszym postępowaniu podmiotowych środków dowodowych na potwierdzenie braku podstaw do wykluczenia.
7. Zamawiający żąda wskazania przez Wykonawcę, w ofercie, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, oraz podania nazw ewentualnych podwykonawców, jeżeli są już znani.
8. W celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania, Zamawiający może żądać od Wykonawcy odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.
    a) Wykonawca nie jest zobowiązany do złożenia dokumentów, o których mowa w zdaniu pierwszym, jeżeli Zamawiający może uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile Wykonawca wskazał dane umożliwiające dostęp do tych dokumentów.
    b) Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów, o których mowa w zdaniu pierwszym, Zamawiający może żądać od Wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania Wykonawcy.
    c) zapis z lit. b) powyżej stosuje się odpowiednio do osoby działającej w imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.
9. W celu potwierdzenia zgodności oferowanego przez Wykonawcę oprogramowania z wymaganiami określonymi przez Zamawiającego, Wykonawca zobowiązany jest złożyć wraz z ofertą przedmiotowy środek dowodowy:
   opis funkcjonalności oprogramowania antywirusowego oraz oprogramowania do inwentaryzacji sprzętu oferowanego przez Wykonawcę ze wskazaniem wszystkich wymaganych przez Zamawiającego funkcji.
   Zamawiający nie przewiduje możliwości uzupełnienia wskazanego wyżej przedmiotowego środka dowodowego.
10. Dokumenty oraz oświadczenia, o których mowa w niniejszym rozdziale SWZ należy złożyć wraz z ofertą za pośrednictwem Platformy zakupowej dostępnej pod adresem https://platformazakupowa.pl/pn/powiat_leszczynski
11. Szczegółowe zasady dotyczące sporządzania dokumentów i oświadczeń, znajdują się w rozdziale XII SWZ.

IX. Informacje o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami, oraz informacje dotyczące wymagań technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. Osoby uprawnione do komunikowania się z Wykonawcami:

1) **Katarzyna Tyczyńska –** w zakresie procedury postępowania - e-mail: k.tyczynska@powiat-leszczynski.pl
2) **Maciej Hampel –** w zakresie przedmiotu zamówienia – m.hampel@powiat-leszczynski.pl

2. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się w formie elektronicznej za pośrednictwem **platformazakupowa.pl** pod adresem: **https://platformazakupowa.pl/pn/powiat_leszczynski**
3. Postępowanie prowadzone jest w języku polskim.
4. Komunikacja między zamawiającym a wykonawcami, w tym składanie oświadczeń, wniosków, zawiadomień oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem formularza **„Wyślij wiadomość do zamawiającego”** dostępnego na platformazakupowa.pl
5. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego” po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.
6. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem platformazakupowa.pl. **Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji “Komunikaty”.** Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.
7. **Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.**
8. Zamawiający, zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. 2020 poz. 2452) określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl , tj.:
   a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   c) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,
   d) włączona obsługa JavaScript,
   e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   f) szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
   g) oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
9. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   a) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
   b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.

10. **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego").** Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu, ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy Prawo Zamówień Publicznych.
11. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
12. **Zalecenia**
    Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
    1) Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf**
    2) W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
       a) .zip
       b) .7Z
    1) Wśród formatów powszechnych, a **nie występujących w rozporządzeniu występują: .rar .gif .bmp .numbers .pages.** Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.
    2) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
    3) Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na **format .pdf** i opatrzenie ich podpisem kwalifikowanym **PAdES**.
    4) Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
    5) Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów, np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
    6) Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
    7) Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza "Wyślij wiadomość do zamawiającego".
    8) Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
    9) Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
    10) Jeśli wykonawca pakuje dokumenty, np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
    11) Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.

12) Zamawiający zaleca, aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików, co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.

13. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Wniosek należy złożyć, zgodnie z zapisami niniejszego rozdziału SWZ, za pośrednictwem **platformazakupowa.pl** pod adresem https://platformazakupowa.pl/pn/powiat_leszczynski za pomocą formularza "Wyślij wiadomość do zamawiającego".
14. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
15. W przypadku, gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 14, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
16. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępni, bez ujawniania źródła zapytania, za pośrednictwem platformazakupowa.pl, w sekcji „Komunikaty".
17. Zamawiający nie przewiduje zwołania zebrania Wykonawców w celu wyjaśnienia treści SWZ.
18. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni za pośrednictwem platformazakupowa.pl, w sekcji „Komunikaty".

X. Wymagania dotyczące wadium

Zamawiający nie wymaga wniesienia wadium.

XI. Termin związania ofertą

1. Wykonawca będzie związany ofertą przez okres 30 dni, tj. do dnia: **5 lipca 2024 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, określonym w ust. 1, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.
5. Zamawiający, zgodnie z art. 226 ust. 1 pkt 12) ustawy Pzp, odrzuci ofertę, jeżeli Wykonawca nie wyrazi pisemnej zgody na przedłużenie terminu związania ofertą.

XII. Opis sposobu przygotowania oferty

1. Oferta składana elektronicznie musi zostać podpisana elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. W procesie składania oferty na platformie, kwalifikowany podpis elektroniczny, podpis zaufany lub podpis osobisty, Wykonawca powinien złożyć bezpośrednio na dokumencie (na każdym załączonym pliku osobno), który następnie przesyła do systemu (opcja rekomendowana przez platformazakupowa.pl).
2. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym

przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.

3. Ofertę należy:
   a) sporządzić w **języku polskim**, dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski;
   b) złożyć, pod rygorem nieważności, przy użyciu środków komunikacji elektronicznej, tzn. za pośrednictwem platformazakupowa.pl,
   c) podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym albo podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.
4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać wymogi rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku.
5. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny, Zamawiający wymaga dołączenia odpowiedniej ilości plików, tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
6. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu do składania ofert **zmienić lub wycofać ofertę**. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
7. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe podlegać będzie odrzuceniu.
8. Zgodnie z definicją dokumentu elektronicznego z art. 3 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
9. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB, natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
10. Dokumenty składane wraz z ofertą (formularz ofertowy stanowiący **załącznik nr 2 do SWZ**):
    1) opis funkcjonalności oprogramowania antywirusowego oraz oprogramowania do inwentaryzacji sprzętu oferowanego przez wykonawcę(**załącznik nr 1 do SWZ**),
    2) oświadczenie Wykonawcy o niepodleganiu wykluczeniu z postępowania (**załącznik nr 3 do SWZ**);
    3) pełnomocnictwo upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik lub pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
    4) oświadczenie Wykonawców wspólnie ubiegających się o zamówienie, w przypadku wspólnego ubiegania się przez Wykonawców o udzielenie zamówienia (**załącznik nr 4 do SWZ**).

Oświadczenia i dokumenty, o których mowa powyżej należy złożyć, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.

11. **Sposób sporządzenia oraz przekazania dokumentów oraz oświadczeń**
    Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art.117 ust 4 ustawy Pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust 3 ustawy Pzp, przedmiotowe środki dowodowe, pełnomocnictwo sporządza się w postaci

elektronicznej, w formatach danych określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2021 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. 2017, poz. 2247), z uwzględnieniem rodzaju przekazywanych danych.

12. W przypadku, gdy dokumenty elektroniczne w postępowaniu, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.
13. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski. Zamawiający nie wyraża zgody na złożenie oferty, oświadczeń oraz innych dokumentów w jednym z języków powszechnie używanych w handlu międzynarodowym.

XIII. Sposób oraz termin składania i otwarcia ofert

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/powiat_leszczynski do dnia **6 czerwca 2024 roku do godz. 10:00.**
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
3. Po wypełnieniu formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl.
5. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 1 oraz ust. 2 Pzp, gdzie zaznaczono, iż oferty oraz oświadczenie, o którym mowa w art. 125 ust. 1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
6. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
7. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
8. Otwarcie ofert nastąpi w dniu **6 czerwca 2024 roku o godz. 10:15** przy użyciu systemu teleinformatycznego w siedzibie Zamawiającego.
9. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
10. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
11. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
12. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
    1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;

2) cenach lub kosztach zawartych w ofertach.

13. Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji „Komunikaty."

XIV. Opis sposobu obliczenia ceny

1. Wykonawca zobowiązany jest podać w formularzu ofertowym cenę jednostkową brutto za **jedną licencję oprogramowania, przez** którą rozumie się: licencję programu antywirusowego i oprogramowania do inwentaryzacji sprzętu oraz wdrożenie, szkolenie z zakresu obsługi oprogramowania i konsultacje serwisowe po wdrożeniu oprogramowania. Cena jednostkowa musi zatem obejmować pełny zakres przedmiotu zamówienia za pojedynczą jednostkę ilości zamówienia.
2. Cena ofertowa musi być podana w złotych polskich (PLN) cyfrowo i słownie, z dokładnością do drugiego miejsca po przecinku, zgodnie z zasadami rachunkowości.
3. W formularzu ofertowym należy podać również łączną cenę brutto za cały zakres przedmiotu zamówienia (wartość wszystkich licencji oprogramowania wraz z wdrożeniem, szkoleniem i konsultacjami po wdrożeniu oprogramowania).
4. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2021 r., poz. 685), dla celów zastosowania kryterium ceny Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.
5. W ofercie, o której mowa w ust. 3, Wykonawca ma obowiązek:
   1) poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
   2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
   3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
   4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.
6. Jeżeli zaoferowana cena, lub ich istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia lub budzą wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, Zamawiający żąda od wykonawcy wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu, lub ich istotnych części składowych.
7. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
8. Rozliczenia finansowe pomiędzy Zamawiającym a Wykonawcą będą prowadzone w złotych polskich.

XV. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Zamawiający dokona oceny ofert niepodlegających odrzuceniu w oparciu o wskazane niżej kryteria.
2. Wartość wagowa wyrażona w procentach jest równa wartości wyrażonej w punktach, tj. 1% = 1 pkt.
3. Kryteria oceny ofert i ich znaczenie oraz opis sposobu oceny ofert:

   1) **cena brutto oferty – waga kryterium 60% (pkt) [P_C]**

Kryterium „cena brutto oferty" obejmuje cenę jednostkową brutto za jedną licencję oprogramowania zgodnie z rozdziałem XIV. ust. 1; punktowo będzie oceniane w skali 0-60 pkt; liczba punktów w powyższym kryterium liczona będzie według wzoru:

$$P_C = \frac{\text{najniższa oferowana cena brutto}}{\text{cena brutto badanej oferty}} \times 60 \text{ pkt}$$

2) **termin wykonania zamówienia – waga kryterium 40% (pkt) [P_T]**

Minimalny wymagany przez Zamawiającego termin wykonania przedmiotu zamówienia wynosi 3 dni od dnia podpisania umowy, a maksymalny 12 dni. Termin wykonania należy zadeklarować w dniach, licząc od dnia podpisania umowy.

Zamawiający przyzna punktację za powyższe kryterium w następujący sposób:
a) oferta z terminem wykonania wynoszącym 3 dni i krótszym otrzyma 40 pkt,
b) oferta z terminem wykonania wynoszącym 7 dni otrzyma 20 pkt,
c) oferta z terminem wykonania wynoszącym 12 dni otrzyma 0 pkt.

Maksymalna liczba punktów w ramach niniejszego kryterium wynosi 40.

Uwagi:
Brak deklaracji terminu wykonania w formularzu ofertowym, bądź zaoferowanie terminu dłuższego niż maksymalny [tj. 12 dni], skutkować będzie odrzuceniem oferty w trybie art. 226 ust. 1 pkt 5 Pzp. Jeżeli natomiast wykonawca zadeklaruje termin krótszy niż minimalny [tj. 3 dni] dla celów porównania złożonych ofert, przyjęty zostanie termin 3 dni, natomiast w treści umowy w sprawie zamówienia publicznego – zgodnie z deklaracją zawartą w ofercie.
Podany termin wykonania będzie wiążący dla Wykonawcy na etapie realizacji zamówienia.

4. Maksymalna liczba punktów jaką Zamawiający może przyznać Wykonawcy wynosi 100 pkt. Całkowita ocena punktowa [P] złożonej i niepodlegającej odrzuceniu oferty składa się z dwóch elementów, które w przypadku otrzymania maksymalnej ilości punktów w każdym z kryteriów pozwalają na uzyskanie 100 pkt:

$$P = P_C + P_T$$

P_C – oznacza punkty w kryterium „cena brutto"

P_T – oznacza punkty w kryterium „termin wykonania zamówienia"

5. Za najkorzystniejszą ofertę uznana zostanie oferta, która odpowiada wszystkim wymaganiom określonym w ustawie Pzp oraz w niniejszej specyfikacji i otrzymała najwyższą liczbę punktów (suma liczby punktów uzyskanych w poszczególnych kryteriach wyboru ofert określonych w niniejszej SWZ).
6. Dla potrzeb oceny ofert, Zamawiający obliczy przyznane Wykonawcom punkty z dokładnością do dwóch miejsc po przecinku.
7. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

8. Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością negocjacji ofert w zakresie kryteriów oceny ofert, celem ich ulepszenia.
   W tym przypadku:
   1) Zamawiający przekaże Wykonawcom informacje, o których mowa w art. 287 ust. 3 ustawy Pzp.
   2) Zamawiający zaprosi do negocjacji maksymalnie **trzech Wykonawców**, których oferty nie podlegały odrzuceniu i którzy otrzymali najwyższą punktację wg kryteriów oceny ofert, z zastrzeżeniem art. 289 ust. 3 ustawy Pzp.
   3) Po zakończeniu negocjacji (charakter poufny) Zamawiający zaprosi Wykonawców do złożenia ofert dodatkowych w terminie 5 dni od dnia przekazania zaproszenia.
   4) Zamawiający dokona oceny ofert dodatkowych zgodnie z ust. 5.

XVII. Informacja o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zgodnie z art. 253 ust 1 Pzp poinformuje równocześnie Wykonawców o:
   1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
   2) Wykonawcach, których oferty zostały odrzucone,
   – podając uzasadnienie faktyczne i prawne.
2. Zamawiający udostępni niezwłocznie informacje, o których mowa w ust. 1 pkt 1 na stronie internetowej: **https://platformazakupowa.pl/pn/powiat_leszczynski** w sekcji „Komunikaty."
3. Zamawiający może nie ujawniać informacji, o których mowa w ust. 1 pkt 1, jeżeli ich ujawnienie byłoby sprzeczne z ważnym interesem publicznym.
4. Zamawiający zawrze umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 Pzp, w terminie nie krótszym niż **5 dni** od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej.
5. Zamawiający zawrze umowę w sprawie zamówienia przed upływem terminu, o którym mowa w ust. 4, jeżeli w niniejszym postępowaniu zostanie złożona tylko jedna oferta.
6. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający może zażądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych Wykonawców.
7. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.
8. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
9. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.
10. W przypadku wybrania oferty Wykonawcy zamierzającego realizować zamówienie z udziałem Podwykonawców mają zastosowanie przepisy rozdziału XVIII SWZ.

XVIII. Wymagania i informacje dotyczące umowy o podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.
2. Zamawiający żąda wskazania przez Wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez Wykonawcę firm podwykonawców, jeżeli są już znane (**Załącznik nr 2 do SWZ**).
3. W przypadku, o którym mowa w ust. 2 Zamawiający będzie badać, czy nie zachodzą wobec podwykonawcy niebędącego podmiotem udostępniającym zasoby, podstawy wykluczenia, o których mowa w art. 108 ust. 1 oraz w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. w celu przeciwdziałania wspieraniu agresji Federacji Rosyjskiej na Ukrainę rozpoczętej w dniu 24 lutego 2022 r. (Dz.U. 15 z 2022 r. poz. 835). Wykonawca przedstawia, oświadczenie, o którym mowa art. 125 ust. 1 ustawy Pzp dotyczące tego podwykonawcy.
4. W przypadku, o którym mowa w ust. 3, jeżeli wobec podwykonawcy zachodzą podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił tego podwykonawcę pod rygorem niedopuszczenia podwykonawcy do realizacji części zamówienia.
5. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
6. Zapisy niniejszego rozdziału SWZ nie naruszają praw i obowiązków Zamawiającego, Wykonawcy, podwykonawcy i dalszego podwykonawcy wynikających z przepisów art. 6471 ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny.

XIX. Istotne dla stron postanowienia umowy

1. Zamawiający zawrze umowę w sprawie zamówienia na warunkach określonych we wzorze umowy, który stanowi załącznik nr 5 do SWZ.
2. Zamawiający przewiduje możliwość istotnych zmian postanowień umowy dotyczących:
   1) aktualizacji danych Wykonawcy i Zamawiającego poprzez: zmianę nazwy firmy, zmianę adresu siedziby, zmianę formy prawnej Wykonawcy itp.,
   2) zmiany osób reprezentujących strony oraz innych osób z nazwiska wymienionych w umowie,
   3) dostosowania umowy do zmian powszechnie obowiązujących przepisów prawa mających wpływ na realizację przedmiotu zamówienia,
3. Warunki dokonania zmian:
   1) strona występująca o zmianę postanowień umowy zobowiązana jest do udokumentowania zaistnienia okoliczności, na które powołuje się, jako podstawę zmiany umowy,
   2) wniosek o zmianę postanowień umowy musi być sporządzony na piśmie,
   3) wniosek, o którym mowa w pkt. 2 musi zawierać:
      a) opis propozycji zmiany,
      b) uzasadnienie zmiany,
      c) opis wpływu zmiany na warunki realizacji umowy.
   4) zmiana umowy może nastąpić wyłącznie w formie pisemnego aneksu pod rygorem nieważności.

XX. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia

1. Wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp, przysługują środki ochrony prawnej określone w Dziale IX ustawy Pzp.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na

listę, o której mowa w art. 469 pkt 15 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.

3. Odwołanie przysługuje na:
   1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania wykonawców lub konkursie, w tym na projektowane postanowienie umowy;
   2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, o zawarcie umowy ramowej, dynamicznym systemie zakupów, systemie kwalifikowania wykonawców lub konkursie, do której zamawiający był obowiązany na podstawie ustawy;
   3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.
4. Odwołanie wnosi się do Prezesa Izby.
5. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
6. Odwołanie wnosi się w terminie:
   1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
   2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.
8. Odwołanie w przypadkach innych niż określone w ust. 6 i 7 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
9. Jeżeli Zamawiający nie przesłał Wykonawcy zawiadomienia o wyborze oferty najkorzystniejszej odwołanie wnosi się nie później niż w terminie:
   1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania,
   2) miesiąca od dnia zawarcia umowy, jeżeli Zamawiający nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania.
10. Zamawiający przesyła niezwłocznie, nie później niż w terminie 2 dni od dnia otrzymania, kopię odwołania innym Wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli odwołanie dotyczy treści ogłoszenia o zamówieniu lub dokumentów zamówienia, zamieszcza ją również na stronie internetowej, na której jest zamieszczone ogłoszenie o zamówieniu lub są udostępniane dokumenty zamówienia, wzywając Wykonawców do przystąpienia do postępowania odwoławczego.
11. Wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje, i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje.
12. Zgłoszenie przystąpienia doręcza się Prezesowi Izby, a jego kopię przesyła się Zamawiającemu oraz Wykonawcy wnoszącemu odwołanie. Do zgłoszenia przystąpienia dołącza się dowód przesłania kopii zgłoszenia przystąpienia Zamawiającemu oraz Wykonawcy wnoszącemu odwołanie.
13. Szczegółowe zasady postępowania po wniesieniu odwołania określają stosowne przepisy Działu IX ustawy Pzp.

14. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
15. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego o apelacji, jeżeli przepisy Działu IX Rozdziału 3 ustawy Pzp nie stanowią inaczej.
16. Skargę wnosi się do Sądu Okręgowego w Warszawie – sądu zamówień publicznych, zwanego dalej „sądem zamówień publicznych", za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe jest równoznaczne z jej wniesieniem.
17. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.
18. Na zasadach określonych w art. 590 ustawy Pzp od wyroku sądu lub postanowienia kończącego postępowanie w sprawie przysługuje skarga kasacyjna do Sądu Najwyższego.

XXI. Informacje dodatkowe

1. Zamawiający informuje, że nie przewiduje możliwości udzielenia dotychczasowemu Wykonawcy zamówień, o których mowa w art. 214 ust. 1 pkt 8 ustawy Pzp.
2. Zamawiający nie dopuszcza składania ofert wariantowych.
3. Zamawiający informuje, że nie przewiduje zawarcia umowy ramowej.
4. Zamawiający informuje, że nie przewiduje złożenia oferty w postaci katalogów elektronicznych.
5. Zamawiający informuje, że nie przewiduje aukcji elektronicznej.
6. Zamawiający informuje, że nie przewiduje ustanowienia dynamicznego systemu zakupów.
7. Zamawiający informuje, że nie przewiduje zwrotu kosztów udziału w postępowaniu.
8. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 ustawy Pzp.
9. Zamawiający nie określa dodatkowych wymagań związanych z zatrudnianiem osób, o których mowa w art. 96 ust. 2 pkt 2 ustawy Pzp.
10. Zamawiający informuje, że nie przewiduje możliwości udzielania zaliczek na poczet wykonania zamówienia.
11. Zamawiający informuje, że nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.
12. Zamawiający informuje, że przed wszczęciem przedmiotowego postępowania nie przeprowadzono wstępnych konsultacji rynkowych.

13. Klauzula informacyjna z art. 13 RODO do zastosowania przez zamawiającego w celu związanym z postępowaniem o udzielenie zamówienia publicznego

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. Urz. UE L 119 z 04.05.2016, str. 1 ze zm.), dalej „RODO", Zamawiający informuje, że:

1) administratorem Pani/Pana danych osobowych jest Starosta Leszczyński, Pl. Kościuszki 4B, 64-100 Leszno*;*
2) w sprawach związanych z Pani/Pana danymi proszę kontaktować się z inspektorem ochrony danych osobowych w Starostwie Powiatowym w Lesznie – kontakt iod@powiat-leszczynski.pl, 65 529-68-36;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz

zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywający na Starostwie Powiatowym w Lesznie jako jednostce sektora finansów publicznych;

4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (tj. Dz. U. z 2021 r., poz. 1129 ze zm.), dalej „ustawa Pzp";
5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, 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 ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
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 Pan/Pani zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia 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 w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników);
   c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem 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, o której mowa w art. 77 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.

Starostwo Powiatowe w Lesznie przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 13 lub 14 RODO wobec osób fizycznych, od których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od Wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.

XXII. Integralną częścią specyfikacji warunków zamówienia są następujące załączniki:

1. Załącznik nr 1 – Opis przedmiotu zamówienia /Opis funkcjonalności oprogramowania antywirusowego oraz oprogramowania do inwentaryzacji sprzętu oferowanego przez Wykonawcę
2. Załącznik nr 2 – Formularz ofertowy
3. Załącznik nr 3 – Wzór oświadczenia o niepodleganiu wykluczeniu
4. Załącznik nr 4 – Wzór oświadczenia Wykonawców wspólnie ubiegających się o udzielenie zamówienia
5. Załącznik nr 5 – Wzór umowy

Leszno, dnia 20 maja 2024 r.

Zatwierdzam:

STAROSTA
/-/ Maciej Wiśniewski

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia
Opis funkcjonalności oprogramowania antywirusowego oraz oprogramowania do inwentaryzacji sprzętu oferowanego przez Wykonawcę

……..
(producent, pełna nazwa oprogramowania oferowanego przez Wykonawcę)

Opis funkcjonalności oprogramowania antywirusowego oraz oprogramowania do inwentaryzacji sprzętu wymaganej przez Zamawiającego		
Administracja zdalna w chmurze	**TAK***	**NIE**
	*należy potwierdzić spełnianie funkcji poprzez wpisanie „TAK" lub „NIE" w przypadku niespełniania funkcji	
Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.		
Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.		
Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.		
Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.		
Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.		
Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.		
Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.		
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.		
Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez Producenta		
Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.		
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.		
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	**TAK**	**NIE**
Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).		
Rozwiązanie musi wspierać architekturę ARM64.		
Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.		
Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.		
Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.		
Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.		
Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.		
Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.		
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.		
Rozwiązanie musi integrować się z Intel Threat Detection Technology.		
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).		
Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.		
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.		
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.		
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.		
Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • 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, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.		
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.		
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.		
Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.		
Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).		
Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.		

Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.		
Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.		
Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.		
Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.		
Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.		
Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.		
Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.		
Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.		
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	**TAK**	**NIE**
Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.		
Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.		
Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.		
Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych		

typu NAS.		
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.		
Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.		
Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.		
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:	TAK	NIE
Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.		
Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).		
Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.		
Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.		
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.		
Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.		
Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.		
Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.		
Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.		
Dodatkowe wymagania dla ochrony serwerów Linux:	TAK	NIE
Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.		
Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi		

serwera Web.		
Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.		
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	**TAK**	**NIE**
System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.		
System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).		
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.		
Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.		
Ochrona urządzeń mobilnych opartych o system Android	**TAK**	**NIE**
Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.		
Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.		
Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).		
Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.		
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.		

Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.		
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.		
Ochrona serwera pocztowego MS Exchange	**TAK**	**NIE**
Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.		
Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.		
Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.		
Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.		
Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.		
Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum		
Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.		
System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.		
Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.		
Rozwiązanie ma posiadać mechanizm greylisting (szara lista).		
Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.		
Sandbox w chmurze	**TAK**	**NIE**
Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.		
Rozwiązanie musi wykorzystywać do działania chmurę producenta.		
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.		
Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.		
Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.		
Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.		
Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.		
Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.		
Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.		
Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.		
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.		
Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a. Czysty, b. Podejrzany, c. Bardzo podejrzany, d. Szkodliwy.		
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.		
W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.		
Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.		
Ochrona usługi Microsoft 365	**TAK**	**NIE**
Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange		

Online, Onedrive, Sharepoint oraz aplikację Teams.		
Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.		
Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.		
Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.		
Rozwiązanie musi być dostępny w języku polskim.		
Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: a. użytkowników, otrzymujących najwięcej spamu, b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, d. kont użytkowników, które mogę być podejrzane.		
Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.		
Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej: a. jaka ilość wiadomości została przeskanowania, b. wynik skanowania poszczególnej wiadomości, c. czynność podjęta przez rozwiązanie.		
Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: a. zagrożeniach, które zostały wykryte, b. na jakim koncie zostały wykryte, c. jakie zagrożenie zostało wykryte, d. podjętą czynność.		
Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.		
Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.		
Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.		
Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej: a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, b. wprowadzenia białych i czarnych list adresów ochrony Exchange’a		

Online, c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.		
Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.		
Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.		
Funkcja ochrony przed zagrożeniami 0-day 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.		
Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.		
Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.		
Moduł XDR	**TAK**	**NIE**
Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.		
Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.		
Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.		
Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.		
Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.		
Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.		
Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.		
Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.		
Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.		
Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i		

popularność pliku.		
Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.		
Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.		
W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.		
W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.		
Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.		
Konsola administracyjna musi mieć możliwość tagowania obiektów.		
Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.		
Moduł zarządzania podatnościami i aktualizacjami	**TAK**	**NIE**
Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach		
Baza wykrywanych podatności musi zawierać minimum 35000 CVE.		
Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.		
Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.		
Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum: - nazwę aplikacji lub systemu operacyjnego - punktacje CVSS		

- opis wykrytej podatności - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta		
Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.		
Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.		
Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.		
Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.		
Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.		
Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.		
Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.		
Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.		
Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.		
Ochrona poprzez dwuskładnikowe uwierzytelnianie	**TAK**	**NIE**
Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 /2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.		
Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11		
Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.		
Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013/ 2016 / 2019.		
Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 /2015 / 2016.		

Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.		
Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.		
Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.		
Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.		
Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.		
Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).		
Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.		
Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.		
Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.		
Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.		
Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego		
Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.		

*(**podpis elektroniczny** osoby/osób upoważnionej do reprezentowania Wykonawcy)*

Załącznik nr 2 do SWZ

FORMULARZ OFERTOWY

Dane dotyczące Wykonawcy

Nazwa: ***(pełna nazwa Wykonawcy/Wykonawców, w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)***	
Adres:	
Województwo, w którym mieści się siedziba Wykonawcy:	
Nr telefonu/faksu:	
e-mail:	
nr NIP:	
nr REGON:	

Odpowiadając na ogłoszenie o zamówieniu udzielanym w trybie podstawowym z możliwością negocjacji, którego przedmiotem jest **zakup oprogramowania antywirusowego wraz z oprogramowaniem do inwentaryzacji sprzętu w zakresie udostępnienia prawa licencji użytkowania dla Starostwa Powiatowego w Lesznie oraz jednostek organizacyjnych**, zobowiązujemy się wykonać przedmiot zamówienia zgodnie z opisem zawartym w SWZ, za wynagrodzenie:

cena netto……..zł za jedną licencję oprogramowania

(słownie: .....)

podatek VAT……%.....zł

cena brutto……..zł za jedną licencję oprogramowania

(słownie: .....)

Łączna cena brutto za cały zakres przedmiotu zamówienia (wartość wszystkich licencji oprogramowania wraz z wdrożeniem, szkoleniem i konsultacjami po wdrożeniu oprogramowania)……..zł
(słownie: .....)

Kryterium pozacenowe:
termin wykonania zamówienia: **…….. (wpisać ilość dni)**

1. Oświadczamy, że oferowana cena brutto obejmuje wszystkie koszty związane z realizacją zamówienia.
2. Oświadczamy, że zapoznaliśmy się z SWZ i nie wnosimy do niej żadnych zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty.
3. Uważamy się za związanych niniejszą ofertą do terminu związania ofertą wskazanego w SWZ.
4. Oświadczamy, że przedmiot zamówienia zamierzamy wykonać:

sami bez udziału podwykonawców */ z udziałem podwykonawców

W przypadku powierzenia części zamówienia podwykonawcom – Wykonawca wypełnia poniższe:

Wskazanie części zamówienia powierzanej podwykonawcy	Wartość lub procentowa część zamówienia, jaka zostanie powierzona podwykonawcy	Nazwa i adres firmy podwykonawcy

* niepotrzebne skreślić

5. Zawarte w SWZ istotne postanowienia umowy zostały przez nas zaakceptowane i zobowiązujemy się w przypadku udzielenia nam zamówienia do podpisania umowy w miejscu i terminie określonym przez Zamawiającego.
6. Oświadczamy, że niniejsza oferta zawiera na stronach od ……. Do …….informacje stanowiące **tajemnicę przedsiębiorstwa** w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa stanowi **Załącznik nr….** Do oferty.
7. **Rodzaj wykonawcy** (właściwe zaznaczyć):
   - ☐ mikroprzedsiębiorstwo (zatrudniające mniej niż 10 osób i roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów euro),
   - ☐ małe przedsiębiorstwo (zatrudniające mniej niż 50 osób i roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów euro),
   - ☐ średnie przedsiębiorstwo (zatrudniające mniej niż 250 osób i roczny obrót nie przekracza 50 milionów euro lub roczna suma bilansowa nie przekracza 43 milionów euro),
   - ☐ duże przedsiębiorstwo (zatrudniające 250 lub więcej osób i roczny obrót przekracza 50 milionów euro lub roczna suma bilansowa przekracza 43 milionów euro)
8. Załącznikami do niniejszej oferty są:
   1) …..
   2) …..
   3) …..
9. Oświadczam/my, że wypełniłem/wypełniliśmy w imieniu Zamawiającego obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

…… *(miejscowość),* dnia …….. r.

*(**podpis elektroniczny** osoby/osób upoważnionej do reprezentowania Wykonawcy)*

Informacje dla wykonawcy:

1. *Formularz oferty musi być podpisany przez osobę lub osoby uprawnione do reprezentowania Wykonawcy i przedłożony wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.*
2. *W przypadku, gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia następuje np. przez jego wykreślenie).*

Załącznik nr 3 do SWZ

Wykonawca:

……
……
……
(pełna nazwa, adres)

Oświadczenie wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych w postępowaniu o udzielenie zamówienia publicznego prowadzonym **w trybie podstawowym z możliwością negocjacji, którego przedmiotem jest zakup oprogramowania antywirusowego wraz z oprogramowaniem do inwentaryzacji sprzętu w zakresie udostępnienia prawa licencji użytkowania dla Starostwa Powiatowego w Lesznie oraz jednostek organizacyjnych**

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

I. OŚWIADCZENIE WYKONAWCY

1. Oświadczam/my, że nie podlegam/my wykluczeniu z postępowania na podstawie art. 108 ust. 1 Pzp.

2. Oświadczam/my, że zachodzą w stosunku do mnie/nas podstawy wykluczenia z postępowania na podstawie art. …… ustawy Pzp (*podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 ustawy Pzp*).
   Jednocześnie oświadczam/my, że w związku z ww. okolicznością, na podstawie art. 110 ust 2 ustawy Pzp podjąłem/ podjęliśmy następujące środki naprawcze:
   ……

3. Oświadczam/my, że nie podlegam/my wykluczeniu 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. z 2022 r., poz. 835).

II. OŚWIADCZENIE WYKONAWCY DOTYCZĄCE PODWYKONAWCY/ÓW

1. Oświadczam/my, że Podwykonawca/cy …….. nie podlegaj/ją wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam/my, że Podwykonawca/cy …….. nie podlegaj/ją wykluczeniu 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. z 2022 r., poz. 835).

III. OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

…….. *(miejscowość),* dnia …….. r.

*(**podpis elektroniczny** osoby/osób upoważnionej do reprezentowania Wykonawcy)*

Załącznik nr 4 do SWZ

Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia

składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych w postępowaniu o udzielenie zamówienia publicznego prowadzonego **w trybie podstawowym z możliwością negocjacji, którego przedmiotem jest zakup oprogramowania antywirusowego wraz z oprogramowaniem do inwentaryzacji sprzętu w zakresie udostępnienia prawa licencji użytkowania dla Starostwa Powiatowego w Lesznie oraz jednostek organizacyjnych**

Oświadczam, że:

1. Wykonawca ……
   (nazwa i adres Wykonawcy)
   zrealizuje zamówienie w zakresie:
   ……
   ……

2. Wykonawca ……
   (nazwa i adres Wykonawcy)
   zrealizuje zamówienie w zakresie:
   ……
   ……

3. Wykonawca ……
   (nazwa i adres Wykonawcy)
   zrealizuje zamówienie w zakresie:
   ……
   ……

…….. *(miejscowość),* dnia …….. r.

*(**podpis elektroniczny** osoby/osób upoważnionej do reprezentowania Wykonawcy)*

Załącznik nr 5 do SWZ

Wzór umowy

W dniu ….. 2024 r. w Lesznie pomiędzy Powiatem Leszczyńskim, z siedzibą w Lesznie przy Pl. Kościuszki 4B, zwanym dalej Zamawiającym, w imieniu którego działają:

Starosta Leszczyński – Maciej Wiśniewski
Wicestarosta Leszczyński – Rafał Jagodzik

przy kontrasygnacie Skarbnika Powiatu – dr. Marcina Wydmucha
a

firmą …….. z siedzibą w ……. przy ul. ……., NIP: ……., zwaną dalej Wykonawcą, w którego imieniu działa …….

w wyniku postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym z możliwością negocjacji, o którym mowa w art. 275 pkt 2 ustawy z 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2023 r., poz. 1605 ze zm.), zawarta została umowa o następującej treści:

§ 1.

1. Przedmiotem zamówienia jest zakup oprogramowania antywirusowego wraz z oprogramowaniem do inwentaryzacji sprzętu w zakresie udostępnienia prawa licencji użytkowania, wdrożenie oraz przeszkolenie osób odpowiedzialnych za obsługę oprogramowania dla Starostwa Powiatowego w Lesznie oraz jednostek organizacyjnych.
   Ilość licencji: **180**.
   1) Starostwo Powiatowe w Lesznie – 121 licencji
   2) Powiatowe Centrum Pomocy Rodzinie w Lesznie – 10 licencji
   3) Zarząd Dróg Powiatowych – 12 licencji
   4) Specjalny Ośrodek Szkolno-Wychowawczy im. F. Ratajczaka – 20 licencji
   5) Zespół Szkół Specjalnych w Górznie – 2 licencje
   6) Powiatowa Poradnia Psychologiczno-Pedagogiczna – 11 licencji
   7) Środowiskowy Dom Samopomocy w Kąkolewie – 4 licencje.

   Okres udzielenia licencji: 24 miesiące od dnia udzielenia licencji Zamawiającemu.
   Zakres zamówienia obejmuje wdrożenie oprogramowania w formie online lub stacjonarnie oraz przeszkolenie dwóch osób wskazanych przez Zamawiającego. Wymaga się przeprowadzenia dwóch szkoleń autoryzowanych przez producenta w trybie online lub stacjonarnie, zrealizowanych w ośrodku szkoleniowym producenta na terenie kraju. Po wdrożeniu oprogramowania Wykonawca zobowiązany jest zapewnić trzy konsultacje serwisowe zdalnie lub stacjonarnie.
2. Szczegółowy opis przedmiotu zamówienia zawarto w załączniku nr 1 do SWZ.
3. Oprogramowanie oferowane przez Wykonawcę musi wykonywać wszystkie funkcje podane przez Zamawiającego w opisie przedmiotu zamówienia.

§ 2.

1. Wykonawca zobowiązuje się wykonać przedmiot umowy, o którym mowa w § 1. w terminie do **…. dni** od dnia podpisania umowy (zgodnie z deklaracją Wykonawcy złożoną w formularzu ofertowym).
2. Wykonanie przedmiotu umowy potwierdzone zostanie protokołem wykonania zamówienia podpisanym przez obie strony.
3. Podpisanie przez Zamawiającego protokołu wykonania zamówienia nie wyklucza dochodzenia roszczeń z tytułu rękojmi i gwarancji w przypadku wykrycia wad przedmiotu zamówienia w terminie późniejszym.

4. W przypadku stwierdzenia, że przedmiot zamówienia nie jest zgodny z wymaganiami określonymi w SWZ, niniejszą umową oraz ofertą Wykonawcy lub nie funkcjonuje prawidłowo, zostanie sporządzony i podpisany przez Wykonawcę i Zamawiającego protokół rozbieżności, w którym:
   1) zawarty zostanie wykaz stwierdzonych wad lub nieprawidłowości w funkcjonowaniu lub niezgodności przedmiotu zamówienia z niniejszą umową;
   2) określony zostanie termin i sposób usunięcia stwierdzonych wad, nieprawidłowości lub niezgodności.
5. W przypadku, gdy Wykonawca nie stawi się do sporządzenia lub podpisania protokołu rozbieżności w terminie wskazanym przez Zamawiającego, Zamawiający sporządzi taki protokół rozbieżności jednostronnie, zawiadamiając Wykonawcę o tym fakcie oraz wzywając go do usunięcia wad lub nieprawidłowości lub niezgodności w terminach wskazanych w protokole rozbieżności.
6. Jeżeli Wykonawca odmówi usunięcia stwierdzonych wad lub nieprawidłowości lub niezgodności w wyznaczonym terminie lub nie usunie ich w wyznaczonym terminie, Zamawiający może według swego uznania naliczyć karę umowną za zwłokę w wysokości 0,5% wynagrodzenia brutto przysługującego Wykonawcy za każdy rozpoczęty dzień zwłoki albo odstąpić od umowy z winy Wykonawcy bez wyznaczania dodatkowego terminu.

§ 3.

1. Wykonawca oświadcza, że przedmiot umowy jest wolny od braków i wad, w tym wad prawnych.
2. Wykonawca udziela gwarancji na przedmiot umowy w wymiarze 24 miesięcy od daty podpisania protokołu odbioru.
3. Gwarancja obejmuje:
   1) regularne aktualizacje definicji wirusów i oprogramowania antywirusowego;
   2) wsparcie techniczne dostępne w dni robocze, od poniedziałku do piątku w godzinach pracy Zamawiającego;
   3) naprawę wszelkich wykrytych błędów i problemów związanych z działaniem oprogramowania.
4. Gwarancja nie obejmuje:
   1) uszkodzeń powstałych w wyniku niewłaściwego użytkowania oprogramowania przez Zamawiającego;
   2) sytuacji, w których Zamawiający dokonał nieautoryzowanych modyfikacji oprogramowania.
5. Wszelkie problemy związane z działaniem oprogramowania należy zgłaszać Wykonawcy w dni robocze, telefonicznie lub mailowo:
   1) telefonicznie pod nr: ……..,
   2) e-mailem pod adres: ……
6. Wykonawca zobowiązuje się do:
   1) rozpoczęcia działań naprawczych w ciągu 8 godzin od zgłoszenia usterki.
   2) usunięcia usterki w ciągu 48 godzin od momentu zgłoszenia.
7. W przypadku braku możliwości usunięcia usterki w ciągu 48 godzin, Wykonawca zobowiązuje się do dostarczenia tymczasowego rozwiązania problemu lub, jeśli to konieczne, wymiany oprogramowania na nowe, bez dodatkowych kosztów dla Zamawiającego.
8. W pozostałym zakresie do gwarancji i rękojmi mają zastosowanie przepisy Kodeksu cywilnego.

§ 4.

1. Osoby odpowiedzialne za realizację niniejszej umowy:
   - po stronie Zamawiającego – Maciej Hampel – tel. 65 529-68-36.
   - po stronie Wykonawcy – …….. – tel. ……..
2. Osoby są uprawnione do podpisywania protokołów, o których mowa w § 2.

§ 5.

1. Zamawiający zapłaci Wykonawcy za przedmiot umowy określony w § 1. niniejszej umowy ……. **zł brutto** (słownie złotych: ……..).
2. Podstawą do wystawienia faktury będzie protokół wykonania zamówienia podpisany przez strony bez uwag.
3. Zapłata nastąpi przelewem w ciągu 14 dni od otrzymania prawidłowej i zgodnej z niniejszą umową faktury przez Zamawiającego.
4. W przypadku otrzymania faktury nieprawidłowej albo niezgodnej z umową Zamawiającemu przysługuje prawo odmowy jej zapłaty. Zamawiający odeśle taką fakturę Wykonawcy.
5. Dane do wystawienia faktury: Powiat Leszczyński, Pl. Kościuszki 4B, 64-100 Leszno, NIP: 697-229-47-65.
6. W kwotę wynagrodzenia Wykonawcy podaną w ust. 1 niniejszego paragrafu zostały wliczone wszelkie koszty związane z realizacją przedmiotu zamówienia, jakie będzie ponosił Wykonawca, zgodnie z umową, jej załącznikami, oraz postanowieniami SWZ, jak i ewentualne ryzyko wynikające z okoliczności, których nie można było przewidzieć w chwili składania oferty.
7. Niedoszacowanie, pominięcie oraz brak rozpoznania zakresu przedmiotu zamówienia nie może być podstawą do żądania zmiany wynagrodzenia określonego w ust. 1 niniejszego paragrafu.
8. Podana w ofercie i umowie cena jest ostateczna i nie może ulec zmianie w trakcie trwania umowy.
9. Datą spełnienia świadczenia jest data obciążenia rachunku bankowego Zamawiającego.
10. Wykonawca nie może przenieść wierzytelności wobec Zamawiającego wynikających z niniejszej umowy na osobę trzecią bez uprzedniej pisemnej zgody Zamawiającego, i to pod rygorem nieważności.

§ 6.

1. Wykonawca jest zobowiązany do zapłacenia Zamawiającemu kar umownych w następujących przypadkach:
    1) 10% wartości wynagrodzenia brutto przysługującego Wykonawcy w przypadku, jeśli Zamawiający albo Wykonawca odstąpi od niniejszej umowy w całości lub części albo ją rozwiąże z przyczyn leżących po stronie Wykonawcy,
    2) 0,5% wartości wynagrodzenia brutto przysługującego Wykonawcy za każdy rozpoczęty dzień zwłoki w wykonaniu umowy,
    3) 0,5% wartości wynagrodzenia brutto przysługującego Wykonawcy za każdy rozpoczęty dzień zwłoki w usunięciu wad lub braków stwierdzonych przy odbiorze przedmiotu umowy, liczonego od dnia wyznaczonego na usunięcie wad;
    4) niedotrzymania terminów procedury reklamacyjnej określonych dla w § 3. ust. 7 umowy, Wykonawca zobowiązuje się do zapłaty kary umownej w wysokości 0.5% wartości zamówienia za każdy dzień zwłoki.
2. Kary, o których mowa w ust. 1 Wykonawca zapłaci na wskazany przez Zamawiającego rachunek bankowy przelewem, w terminie 14 dni kalendarzowych od dnia doręczenia mu żądania Zamawiającego zapłaty takiej kary umownej.
3. Niezależnie od ww. kar Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania do wysokości faktycznie poniesionej straty w związku z niewykonaniem lub nienależytym wykonaniem zamówienia.
4. Zamawiający jest uprawniony do potrącenia kwot kar umownych z wynagrodzenia należnego Wykonawcy, na co Wykonawca wyraża zgodę.
5. Łączny limit kar umownych, jakich Zamawiający może żądać od Wykonawcy ze wszystkich tytułów przewidzianych w ust. 2, wynosi 30% wynagrodzenia umownego brutto określonego w § 5 ust. 1 Umowy.

§ 7.

1. Zmiana umowy wymaga formy pisemnej pod rygorem nieważności.

2. Zamawiający przewiduje możliwość istotnych zmian postanowień umowy dotyczących:
   1) aktualizacji danych Wykonawcy i Zamawiającego poprzez: zmianę nazwy firmy, zmianę adresu siedziby, zmianę formy prawnej Wykonawcy itp.,
   2) zmiany osób reprezentujących strony oraz innych osób z nazwiska wymienionych w umowie,
   3) dostosowania umowy do zmian powszechnie obowiązujących przepisów prawa mających wpływ na realizację przedmiotu zamówienia.
4. Warunki dokonania zmian:
   1) strona występująca o zmianę postanowień umowy zobowiązana jest do udokumentowania zaistnienia okoliczności, na które powołuje się, jako podstawę zmiany umowy,
   2) wniosek o zmianę postanowień umowy musi być sporządzony na piśmie,
   3) wniosek, o którym mowa w pkt. 2 musi zawierać:
      a) opis propozycji zmiany,
      b) uzasadnienie zmiany,
      c) opis wpływu zmiany na warunki realizacji umowy.
   4) zmiana umowy może nastąpić wyłącznie w formie pisemnego aneksu pod rygorem nieważności.

§ 8.

W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy kodeksu cywilnego, a ewentualne sprawy sporne będzie rozstrzygał sąd powszechny właściwy dla miejsca Zamawiającego.

§ 9.

Umowa została zawarta w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Zamawiający **Wykonawca**