Zespół Opieki Zdrowotnej we Włoszczowie

– Szpital Powiatowy im. Jana Pawła II

ul. Żeromskiego 28, 29-100 Włoszczowa

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ) pn:

„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II”

Znak sprawy:

09/09/2023

Włoszczowa, dnia 21.09.2023 rok

I. Zamawiający:

Zespół Opieki Zdrowotnej we Włoszczowie – Szpital Powiatowy im. Jana Pawła II
ul. Żeromskiego 28, 29-100 Włoszczowa
telefon 041 38 83 828,
adres e-mail: **zaopatrzenie@zozwloszczowa.pl**
NIP 656 –18 – 55 908, REGON 000304295
Adres strony internetowej Zamawiającego: http://www.zozwloszczowa.pl

Godziny urzędowania: poniedziałek – piątek od 7:30 do 15:05

II. Adres strony internetowej, na której jest prowadzone postępowanie i na której będą udostępnione zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia

Adres platformy, za pomocą której należy złożyć ofertę oraz na której udostępnione będą zmiany i wyjaśnienia treści specyfikacji warunków zamówienia (SWZ) oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia: https://platformazakupowa.pl/pn/zoz_wloszczowa

III. Tryb udzielenia zamówienia publicznego:

1. Postępowanie prowadzone jest w trybie podstawowym bez negocjacji, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 ze zm.), zwanej dalej „ustawa Pzp", oraz aktów wykonawczych do niej, o wartości zamówienia poniżej progu unijnego.
2. W sprawach nieuregulowanych zapisami niniejszej SWZ, stosuje się przepisy wspomnianej ustawy oraz aktów wykonawczych wydanych na podstawie ustawy.

IV. Rodzaj zamówienia:

Dostawa ***oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych*** dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II.

V. Przedmiot zamówienia:

1. Przedmiotem zamówienia jest *dostawa* ***oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych wraz z wykonaniem usług podnoszących bezpieczeństwo systemów IT w ramach środków pochodzących z Funduszu Przeciwdziałania COVID-19 - podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców (Zarządzenie nr 8/2023/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 16 stycznia 2023 r. ze zmianami)***, w tym:
   a) Dostawa systemu kopii zapasowych wraz ze sprzętem i konfiguracją
   b) Dostawa licencji antywirusowych wraz z Endpoint Detection and Response
   c) Wykonanie usług wdrożeniowych w zakresie dostarczanego oprogramowania
   d) Wsparcie powdrożeniowe na okres 5 lat
   e) Wykonanie usług szkoleniowych dla pracowników Zamawiającego.

2. **Szczegółowy opis przedmiotu zamówienia - stanowiący załącznik nr 1 do SWZ** określa asortyment, ilości oraz wymagania jakościowe i techniczne przedmiotu zamówienia.

3. Jeśli w przedmiocie zamówienia Zamawiający opisał materiały, urządzenia, technologie ze wskazaniem konkretnych znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, to należy je traktować jako przykładowe i Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych stosownie do postanowień 99 ust 5 i 6 Pzp. Kryterium równoważności stosowanym w celu oceny równoważności zaoferowanych rozwiązań jest spełnienie przez zaoferowane rozwiązania, co najmniej takich samych lub lepszych parametrów technicznych i funkcjonalnych, nie obniżających określonych standardów, niż te które wynikają z opisu przedmiotu zamówienia. Wykonawca oferujący rozwiązania równoważne obowiązany jest udowodnić na etapie składania oferty, że oferowane rozwiązanie posiada parametry i cechy, o których mowa w zdaniu poprzednim. Brak wskazania proponowanych odpowiedników i opisu dotyczącego właściwości zastosowanych odpowiedników stanowi podstawę do odrzucenia oferty – art. 226 ust. 1 pkt 5) Ustawy Prawo Zamówień Publicznych.

4. **Kod CPV**

   48000000-8 - Pakiety oprogramowania i systemy informatyczne
   48800000-6 Systemy i serwery informacyjne

5. Zadanie dofinansowane ze środków Funduszu Przeciwdziałania COVID-19 w ramach zarządzenia Prezesa NFZ nr 8/2023/BBIICD ze zmianami na podstawie umowy Nr 14/NFZ13-ZBIiCD.4033.32.2023 r. zawartej z Narodowym Funduszem Zdrowia.

VI. Opis części zamówienia:

1. Zamawiający dopuszcza składanie ofert częściowych na poszczególne pakiety **nr 1** - dostawa wraz z instalacją sprzętu z oprogramowaniem i **nr 2** - dostawy licencji oprogramowania komputerowego (pakiety nie podlegają podziałowi).
2. Oferty można składać w odniesieniu do jednego lub większej liczby pakietów**.**
3. W przypadku, gdy oferta jednego wykonawcy, złożona na więcej niż jeden pakiet niniejszego postępowania, okaże się najkorzystniejsza, Zamawiający zawrze jedną umowę na realizację zamówienia publicznego.

VII. Informacja o przedmiotowych środkach dowodowych

W celu potwierdzenia zgodności oferowanych dostaw z wymaganiami określonymi w opisie przedmiotu zamówienia związanymi z realizacją zamówienia, Zamawiający nie żąda złożenia wraz z ofertą przedmiotowych środków dowodowych.

VIII. Informacje o przewidywanych zamówieniach podobnych, o których mowa w art. 214 ust. 1 pkt 7) i 8):

Zamawiający nie przewiduje udzielenia zamówień podobnych.

IX. Pozostałe informacje:

1. Zamawiający nie dopuszcza składania ofert wariantowych.
2. Zamawiający nie przewiduje rozliczenia w walutach obcych.
3. Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.
4. Zamawiający nie wymaga złożenia ofert w postaci katalogów elektronicznych.
5. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej.
6. Zamawiający nie przewiduje zawarcia umowy ramowej.
7. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
8. Zamawiający nie zamierza ustanowić dynamicznego systemu zakupów.
9. Zamawiający nie przewiduje przeprowadzenia wizji lokalnej przez Wykonawców oraz udostępnienia w siedzibie Zamawiającego do sprawdzenia dokumentów niezbędnych do realizacji zamówienia.
10. Zamawiający nie przewiduje szczegółowego określania w opisie przedmiotu zamówienia wymagań związanych z realizacją zamówienia, o których mowa w art. 94 ustawy Pzp.
11. Zamawiający nie stawia wymagań w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt. 2 ustawy Pzp.
12. Zamawiający nie stawia wymagań w zakresie zatrudnienia na podstawie stosunku pracy w okolicznościach, o których mowa w art. 95 ustawy Pzp.

X. Termin realizacji przedmiotu zamówienia:

Realizacja zamówienia - w terminie do 15 dni od dnia zawarcia umowy - **jest to termin maksymalny realizacji zamówienia dla obu pakietów**.

W przypadku, gdy w kryterium czas wdrożenia systemu kopii zapasowych dla pakietu nr 1 lub czas dostawy licencji dla pakietu nr 2 - Wykonawca zaproponuje krótszy termin, to w ramach umowy będzie zobowiązany do realizacji umowy w zaproponowanym przez siebie terminie.

XI. Warunki udziału w postępowaniu, podstawy wykluczenia, wykaz podmiotowych środków dowodowych.

XI.I W postępowaniu o udzielenie zamówienia mogą wziąć udział Wykonawcy, którzy spełniają warunki określone w art. 57 ustawy Pzp w zw. z art. 112 ust. 2 ustawy Pzp, tj.:

1) nie podlegają wykluczeniu;

2) spełniają warunki udziału w postępowaniu, dotyczące:

a) zdolności do występowania w obrocie gospodarczym

Zamawiający nie ustala szczegółowego warunku udziału w Postępowaniu.

b) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej

Zamawiający nie ustala szczegółowego warunku udziału w Postępowaniu.

c) sytuacji ekonomicznej lub finansowej

Zamawiający nie ustala szczegółowego warunku udziału w Postępowaniu.

d) zdolności technicznej lub zawodowej

Wykonawca spełni warunek, jeżeli wykaże, że:

- Dla pakietu nr 1 - w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, dostarczył sprzęt i wdrożył system kopii zapasowych o wartości minimum 200 000,00 zł.

- Dla pakietu nr 2 - w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, dostarczył licencje o wartości minimum 50 000,00 zł.

W przypadku złożenia przez Wykonawców dokumentów zawierających dane wyrażone w innych walutach niż PLN, Zamawiający jako kurs przeliczeniowy waluty przyjmie średni kurs Narodowego Banku Polskiego (NBP) obowiązujący w dniu opublikowania ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej lub Biuletynie Informacji Publicznej. Jeżeli w dniu publikacji ogłoszenia o zamówieniu NBP nie opublikuje informacji o średnim kursie walut, Zamawiający dokona odpowiednich przeliczeń wg średniego kursu z pierwszego, kolejnego dnia, w którym NBP opublikuje ww. informacje.

XI.II <u>Poleganie na zasobach innych podmiotów</u>

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają dostawy lub usługi, do realizacji których te zdolności są wymagane. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu albo odpowiednio wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.

2. **Zobowiązanie podmiotu udostępniającego zasoby, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby określa w szczególności:**
   1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy lub usługi, których wskazane zdolności dotyczą.

3. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy (**<u>Wykonawca zobowiązany będzie złożyć na wezwanie Zamawiającego zgodnie z art. 274 ust. 1 ustawy</u>**, **<u>podmiotowe środki dowodowe tych podmiotów, dotyczące braku podstaw wykluczenia z postępowania w takim samym zakresie, w jakim zobowiązany jest złożyć te dokumenty sam Wykonawca</u>**).

4. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub zachodzą, wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
5. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

XI.III <u>Podstawy wykluczenia:</u>

1. **Zamawiający wykluczy z postępowania Wykonawcę w przypadkach, o których mowa w art. 108 ust. 1 pkt 1-6 ustawy (obligatoryjne przesłanki wykluczenia) oraz 109 ust. 1 pkt 1 i 4 (fakultatywne przesłanki wykluczenia):**

   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. poz. 769),
      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, 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. Z postępowania o udzielenie zamówienia, w przypadku zamówienia o wartości równej lub przekraczającej wyrażoną w złotych równowartość kwoty dla robót budowlanych – 20 000 000 euro, a dla dostaw lub usług – 10 000 000 euro, wyklucza się także Wykonawcę, który udaremnia lub utrudnia stwierdzenie przestępnego pochodzenia pieniędzy lub ukrywa ich pochodzenie, w związku z brakiem możliwości ustalenia beneficjenta rzeczywistego, w rozumieniu art. 2 ust. 2 pkt 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tj. Dz. U. z 2020 poz. 971 ze zm.).

3. Z postępowania o udzielenie zamówienia wyklucza się również Wykonawcę:

a) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, 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 ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

b) w stosunku, do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;

4. Zamawiający wykluczy także z postępowania Wykonawców, wobec których zachodzą podstawy do wykluczenia o których mowa w 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 tj. Zamawiający wykluczy z postępowania:

a) Wykonawcę wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, ze zm.), zwanego dalej „rozporządzeniem 765/2006”,

i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, ze zm.), zwanego dalej „rozporządzeniem 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 z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego;

b) Wykonawcę, 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 z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego;

c) Wykonawcę, 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 z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

5. W przypadku Wykonawcy wykluczonego na podstawie pkt 4 powyżej Zamawiający odrzuca ofertę takiego Wykonawcy, nie zaprasza go do złożenia oferty wstępnej, oferty podlegającej negocjacjom, oferty dodatkowej, oferty lub oferty ostatecznej, nie zaprasza go do negocjacji, a także nie prowadzi z takim Wykonawcą negocjacji, odpowiednio do trybu stosowanego do udzielenia zamówienia publicznego oraz etapu prowadzonego postępowania o udzielenie zamówienia publicznego.

XI.IV Procedura samooczyszczenia

1. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 ustawy Pzp 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.

2. Zamawiający ocenia, czy podjęte przez wykonawcę czynności, o których mowa w ust. 1, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w ust. 1, nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza wykonawcę.
3. Wykonawca może zostać wykluczony przez zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
4. W celu skorzystania z instytucji ,,samooczyszczenia", Wykonawca zobowiązany jest do wypełnienia stosownych informacji w oświadczeniu stanowiącym załącznik nr 4 a (4 b dla Podmiotu na którego zasoby powołuje się Wykonawca) do SWZ.

XI.V. Wykaz oświadczeń lub dokumentów potwierdzających spełnienie warunków udziału w postępowaniu oraz postaw do wykluczenia - informacje wstępne

Ocena spełniania podstaw wykluczenia z postępowania, zostanie dokonana zgodnie z formułą „podlega – nie podlega”, w oparciu o przedłożone przez Wykonawcę oświadczenie i dokumenty, o których mowa w rozdz. XI.VII.

XI.VI Wykaz oświadczeń lub dokumentów, jakie mają dostarczyć wykonawcy w celu wstępnego potwierdzenia spełnienia warunków udziału w postępowaniu wraz z ofertą

1. **W zakresie wykazania spełniania przez Wykonawcę warunków, o których mowa w art. 57 ustawy Pzp, Wykonawca przedkłada:**
   a) **oświadczenie o spełnianiu warunków udziału w postępowaniu** – podpisane odpowiednio przez osobę (osoby) upoważnioną (upoważnione) do reprezentowania Wykonawcy. Stosowne oświadczenie, Wykonawca składa na wzorze stanowiącym **Załącznik nr 3 a do SWZ;**
   b) **oświadczenie o spełnianiu warunków udziału w postępowaniu** – podpisane odpowiednio przez osobę (osoby) upoważnioną (upoważnione) do reprezentowania Podmiotu na którego zasoby powołuje się Wykonawca. Stosowne oświadczenie, składa się na wzorze stanowiącym **Załącznik nr 3 b do SWZ;**
2. **W zakresie potwierdzenia braku podstaw do wykluczenia z Postępowania w okolicznościach, o których mowa w art. 108 ustawy Pzp oraz art. 109 ust. 1 pkt 1 oraz pkt 4 ustawy Pzp**, Wykonawca przedkłada:
   a) **oświadczenie o braku podstaw do wykluczenia z postępowania –** wypełnione i podpisane odpowiednio przez osobę (osoby) upoważnioną (upoważnione) do reprezentowania Wykonawcy. Stosowne oświadczenie Wykonawca składa na wzorze stanowiącym **Załącznik nr 4 a do SWZ.**
   b) **oświadczenie o braku podstaw do wykluczenia z postępowania –** wypełnione i podpisane odpowiednio przez osobę (osoby) upoważnioną (upoważnione) do

reprezentowania Podmiotu na którego zasoby powołuje się Wykonawca. Stosowne oświadczenie składa się na wzorze stanowiącym **Załącznik nr 4 b do SWZ.**

XI.VII Podmiotowe środki dowodowe (oświadczenia i dokumenty potwierdzające okoliczności, o których mowa w art. 273 ustawy Pzp, składane na wezwanie zamawiającego):

1. Zamawiający wzywa Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, aktualnych na dzień złożenia:
   a) **odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej**, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 109 ust. 1 pkt 4 ustawy;
   b) **oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp**, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:
   - art. 108 ust 1 pkt 1, 3, 4, 5, 6 u. Pzp,

   - art. 109 ust 1 pkt 1 u. Pzp

   Przedmiotowe oświadczenie należy złożyć na formularzu, którego wzór stanowi **załącznik nr 7 do SWZ.**

   c) **oświadczenia wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp**, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tj. Dz. U. z 2021 r. poz. 275), z innym wykonawcą, który złożył odrębną ofertę, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej – **wzór oświadczenia stanowi załącznik nr 6 do SWZ.**
   d) wykazu dostaw/usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie:
   - Dla pakietu nr 1 - w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, dostarczył sprzęt i wdrożył system kopii zapasowych o wartości minimum 200 000,00 zł.

   - Dla pakietu nr 2 - w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, dostarczył licencje o wartości minimum 50 000,00 zł.

   - wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy/usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy/usługi zostały wykonane lub są wykonywane należycie. Dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy/usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy. W przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte

wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy. **Wykaz dostaw/usług stanowi załącznik nr 5 do SWZ.** Wymagane jest wykazanie co najmniej jednego zamówienia dla pakietu do którego zamierza przystąpić Wykonawca.

2. Wykonawca nie będzie obowiązany do złożenia podmiotowych środków dowodowych, potwierdzających spełnianie warunków udziału w postępowaniu lub brak podstaw wykluczenia, jeżeli Zamawiający posiada oświadczenia a wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070) lub podmiotowych środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp.
3. W przypadku wskazania przez Wykonawcę dostępności oświadczeń lub dokumentów, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobierze samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty.
4. W przypadku wskazania przez Wykonawcę oświadczeń lub dokumentów na potwierdzenie braku podstaw wykluczenia lub spełniania warunków udziału w postępowaniu, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający będzie wymagał od Wykonawcy przedstawienia tłumaczenia na język polski wskazanych przez Wykonawcę i pobranych samodzielnie przez Zamawiającego dokumentów.
5. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w:
   1) Rozdziale XI.VII ust. lit. a – odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej – składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że: nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury
6. Dokument, o którym mowa w ust. 1 pkt. 1 lit. a., powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.
7. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 1 pkt. 1 lit. a, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Postanowienia ust. 6 stosuje się odpowiednio.
8. Jeżeli Wykonawca nie złoży oświadczenia, o którym mowa w rozdz. XI.VI SWZ, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 273 ustawy Pzp, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą, wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia, poprawienia w terminie przez siebie

wskazanym, chyba, że mimo ich złożenia oferta Wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.

9. W zakresie nieuregulowanym ustawą Pzp lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy oraz rozporządzenia 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.

XI.VIII Informacja dla wykonawców wspólnie ubiegających się o udzielenie zamówienia (spółki cywilne/konsorcja)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale XI.VI i XI.VII SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. **Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane/dostawy/usługi wykonają poszczególni wykonawcy (załącznik nr 8).**
4. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa z osobna każdy z Wykonawców wspólnie ubiegających się o zamówienie.

XI.IX Podwykonawcy

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

XII. Oferta

XII.I Oświadczenia i dokumenty, jakie powinni dostarczyć Wykonawcy wraz z ofertą.

1. **oświadczenie o spełnianiu warunków udziału w postępowaniu** i braków podstaw do wykluczenia – podpisane odpowiednio przez osobę (osoby) upoważnioną (upoważnione) do reprezentowania Wykonawcy. Stosowne oświadczenie, Wykonawca składa na wzorze **stanowiącym załącznik nr 3 i 4 do SWZ**,
2. wypełniony i podpisany formularz ofertowy (zgodny ze wzorem, **stanowiącym załącznik nr 2 do SWZ**)

zawierający w szczególności: wskazanie oferowanego przedmiotu zamówienia, cenę ryczałtową netto, wartość podatku VAT, łączną cenę ofertową brutto, zobowiązanie dotyczące terminu realizacji zamówienia, oświadczenie o okresie związania ofertą oraz o akceptacji wszystkich postanowień wzoru umowy bez zastrzeżeń,

3. podpisany szczegółowy opis przedmiotu zamówienia, (**stanowiący załącznik nr 1 do SWZ**),
4. w przypadku gdy wykonawcę reprezentuje pełnomocnik – pełnomocnictwo określające zakres umocowania pełnomocnika,
5. w przypadku oferty składanej przez wykonawców, którzy wspólnie ubiegają się o udzielenie zamówienia (w szczególności członków konsorcjum oraz wspólników spółki cywilnej) – aktualny dokument potwierdzający ustanowienie pełnomocnika do reprezentowania w/w wykonawców w postępowaniu lub do reprezentowania w postępowaniu i zawarcia umowy lub umowę regulującą współpracę i zasady reprezentacji podmiotów występujących wspólnie w szczególności umowę spółki cywilnej.
6. Zobowiązanie podmiotu udostępniającego zasoby.

XII.II Opis sposobu przygotowania ofert oraz dokumentów wymaganych przez zamawiającego w SWZ

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane **elektronicznym kwalifikowanym podpisem** lub **podpisem zaufanym** lub **podpisem osobistym**. W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, **kwalifikowany podpis elektroniczny** lub **podpis zaufany** lub **podpis osobisty** Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu.
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. Oferta powinna być:
    a. sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
    b. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
    c. podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione
4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie 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. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
7. 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
8. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje podlegać będzie odrzuceniu.
9. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
10. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
11. Zgodnie z definicją dokumentu elektronicznego z art. 3 ustęp 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.
12. 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.

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

XIII.I. Informacje Ogólne

1. Osobą uprawnioną do kontaktu z Wykonawcami jest:
   Piotr Szczepanowski – tel.: 533 344 295 - pod względem merytorycznym od pn. do pt. w godzinach 9:00 – 14:00;
   Joanna Krzyzińska / Joanna Szwarc – Dział Obsługi Administracyjno-Technicznej-w sprawach proceduralnych tel. 41 3883837 lub 41 3883828 informacje dotyczące postępowania udzielane są od pn. do pt. w godzinach 9:00 – 14:00, e-mail: zaopatrzenie@zozwloszczowa.pl.
2. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/zoz_wloszczowa
3. W celu skrócenia czasu udzielenia odpowiedzi na pytania komunikacja między zamawiającym a wykonawcami w zakresie:
   a) przesyłania Zamawiającemu pytań do treści SWZ;

b) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;
c) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
d) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
e) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dot. treści przedmiotowych środków dowodowych;
f) przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;
g) przesyłania wniosków, informacji, oświadczeń Wykonawcy;
h) przesyłania odwołania/inne

odbywa się za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego".

4. 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.
5. 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.
6. 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.
7. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 31 grudnia 2020r. 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. z 2020r. 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.
8. 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.

9. **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.
10. 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

11. **Formaty danych postaci elektronicznej oświadczeń i dokumentów**

1. **Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z** "OBWIESZCZENIEM PREZESA RADY MINISTRÓW z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".
2. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf**
3. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
   a. .zip
   b. .7Z
4. Wśród formatów powszechnych a **NIE występujących** w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. **Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.**
5. 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.
6. 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.
7. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
8. 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.
9. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.

10. Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza "Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu email.
11. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
12. Ofertę należy przygotować z należytą starannością i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
13. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
14. Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
15. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
16. 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.
17. **Zamawiający informuje, iż w przypadku jakichkolwiek wątpliwości związanych z zasadami korzystania z Platformy, Wykonawca winien skontaktować się z dostawcą tego rozwiązania teleinformatycznego pod nr infolinii +48 22 101 02 02 (infolinia dostępna w dni robocze, w godzinach 8.00-17.00) e-mail: cwk@platformazakupowa.pl**

XIII.II. Złożenie oferty w postępowaniu.

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/zozwloszczowa do dnia 02.10.2023. godziny 10:00.
2. Termin związania ofertą upływa w dniu 31.10.2023 r.
3. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
4. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania".
5. Oferta lub wniosek 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. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu 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

XIII.III. Otwarcie ofert

1. Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert tj. 02.10.2023 r. godzina 11:00.

2. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia 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.

   Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji ,,Komunikaty".
6. W przypadku ofert, które podlegają negocjacjom, zamawiający udostępnia informacje, o których mowa w ust. 5 pkt 2, niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.

   Zgodnie z Ustawą Prawo Zamówień Publicznych Zamawiający nie ma obowiązku przeprowadzania jawnej sesji otwarcia ofert w sposób jawny z udziałem wykonawców lub transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line a ma jedynie takie uprawnienie.

XIV. Dokumentacja przetargowa

Zawartość dokumentacji przetargowej:

Specyfikacja Warunków Zamówienia wraz z załącznikami:

Załącznik nr 1 – szczegółowy opis przedmiotu zamówienia
Załącznik nr 2 - formularz ofertowy;
Załącznik nr 3 (a i b) - oświadczenie o spełnieniu warunków udziału w postępowaniu;
Załącznik nr 4 (a i b) – oświadczenie o braku podstaw do wykluczenia;
Załącznik nr 5 – wzór wykazu dostaw/usług;
Załącznik nr 6 – oświadczenie Grupa Kapitałowa – wzór;
Załącznik nr 7 – oświadczenie dot. aktualności informacji
Załącznik nr 8 – oświadczenie wykonawców;
Załącznik nr 9 – istotne postanowienia umowy.

XV. Wadium:

Zamawiający nie wymaga wniesienia wadium.

XVI. Zabezpieczenie należytego wykonania umowy:

Zamawiający nie wymaga wnoszenia zabezpieczenia należytego wykonania umowy.

XVII. Kryteria oceny ofert:

I. Do oceny ofert przyjmuje się następujące kryteria:

Cena danej części zamówienia brutto – wartość kryterium – **60 %**

Podstawą oceny jest cena zamówienia brutto zaproponowana przez Wykonawcę w formularzu ofertowym (załącznik nr 2 do SWZ).

Kryterium ceny – (Kc).

$$\mathbf{Kc} = \frac{\text{Najniższa łączna cena danej części zamówienia brutto spośród nieodrzuconych ofert}}{\textbf{Łączna cena danej część zamówienia brutto w badanej nieodrzuconej ofercie.}} \textbf{ x 100 x 60\%}$$

Maksymalna ilość punktów do uzyskania w kryterium „Cena" wynosi – 60 pkt. Zamawiający wyliczy liczbę punktów uzyskanych przez poszczególne oferty w oparciu o ww. wzór z dokładnością do dwóch miejsc po przecinku.

W formularzu ofertowym Oferent przedstawi całkowitą wartość netto, podatek VAT oraz wartość brutto. Cena oferty winna zawierać wszelkie koszty związane z dostawą towaru. Jeżeli Wykonawca stosuje rabaty to należy je uwzględnić w cenie oferty.

II **Kryterium czas:**

Dla pakietu nr 1 - czas wdrożenia systemu kopii zapasowych – 40%

Zamawiający wymaga, aby czas wdrożenia systemu kopii zapasowych był nie dłuższy niż 15 dni od daty zawarcia umowy. Wykonawca w formularzu ofertowym może określić krótszy czas wdrożenia systemu kopii zapasowych, za który może uzyskać dodatkowe punkty w przedmiotowym kryterium.

Minimalny czas wdrożenia systemu kopii zapasowych, za który można otrzymać maksymalna liczbę punktów wynosi 5 dni.

Maksymalna ilość uzyskanych punktów w kryterium czas wdrożenia systemu kopii zapasowych wynosi 40 pkt.
Punkty zostaną przyznane wg następujących zasad:

Czas wdrożenia systemu kopii zapasowych w terminie do 5 dni od daty zawarcia umowy	40 punktów
Czas wdrożenia systemu kopii zapasowych powyżej 5 dni do 10 dni od daty zawarcia umowy	20 punktów
Czas wdrożenia systemu kopii zapasowych powyżej 10 do 15 dni od daty zawarcia umowy	0 punktów

Dla pakietu nr 1 - czas dostawy licencji antywirusowych – 40%

Zamawiający wymaga, aby czas dostawy licencji antywirusowych był nie dłuższy niż 15 dni od daty zawarcia umowy. Wykonawca w formularzu ofertowym może określić krótszy czas dostawy, za który może uzyskać dodatkowe punkty w przedmiotowym kryterium.

Minimalny czas dostawy licencji, za który można otrzymać maksymalna liczbę punktów wynosi 5 dni.
Maksymalna ilość uzyskanych punktów w kryterium czas dostawy licencji antywirusowych wynosi 40 pkt.
Punkty zostaną przyznane wg następujących zasad:

Czas dostawy licencji w terminie do 5 dni od daty zawarcia umowy	40 punktów
Czas dostawy licencji powyżej 5 dni do 10 dni od daty zawarcia umowy	20 punktów
Czas dostawy licencji powyżej 10 do 15 dni od daty zawarcia umowy	0 punktów

Oferta najkorzystniejsza:

1. Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą łączną liczbę punktów obliczoną na podstawie zsumowania liczby punktów uzyskanych w poszczególnych kryteriach oceny ofert (cena danej części zamówienia + czas).
2. 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 wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
3. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, zamawiający wybiera ofertę z najniższą ceną lub kosztem.
4. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa powyżej, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych zawierających nową cenę lub koszt.
5. Wykonawcy, składając oferty dodatkowe, nie mogą oferować cen lub kosztów wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
6. **Wszelkie rozliczenia pomiędzy zamawiającym a wykonawcą dokonywane będą wyłącznie w złotych polskich.**

XVIII. Opis sposobu obliczania i podania ceny

Przez cenę – należy rozumieć cenę w rozumieniu art. 3 ust. 1 pkt 1 ustawy z dnia 9 maja 2014 roku, o informowaniu o cenach towarów i usług (tj. Dz. U. z 2019 r. poz. 178)

Zamawiający wymaga by cena ostateczna oferty była podana w złotych polskich brutto – cyfrowo i słownie z dokładnością do dwóch miejsc po przecinku.
Obowiązkiem składającego ofertę jest:

1. Wykonawca uwzględniając wszystkie wymogi, o których mowa w niniejszej Specyfikacji Warunków Zamówienia, powinien w cenie brutto ująć wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania przedmiotu zamówienia oraz uwzględnić inne opłaty i podatki, a także ewentualne upusty i rabaty zastosowane przez Wykonawcę.

2. Cena brutto za realizację zamówienia zostanie przedstawiona w składanej ofercie z dokładnością do 2 miejsc po przecinku (wzór formularz ofertowy załącznik nr 2).
3. Ostateczna cena oferty, obejmuje wartość przedmiotu zamówienia wraz z właściwą zgodną z obowiązującymi przepisami prawa stawką podatku VAT – ewentualny błąd w tym zakresie będzie stanowił podstawę do odrzucenia oferty, jako zawierającej błąd w obliczeniu ceny.
4. Każdy z Wykonawców może zaproponować tylko jedną cenę.

XIX. Odrzucenie oferty

Zamawiający odrzuca ofertę, jeżeli:

1. została złożona po terminie składania ofert;
2. została złożona przez wykonawcę:
   - podlegającego wykluczeniu z postępowania;
   - niespełniającego warunków udziału w postępowaniu;
   - który nie złożył w przewidzianym terminie oświadczenia, o którym mowa w art. 125 ust. 1, lub podmiotowego środka dowodowego, potwierdzających brak podstaw wykluczenia lub spełnianie warunków udziału w postępowaniu, przedmiotowego środka dowodowego, lub innych dokumentów lub oświadczeń;
3. jest niezgodna z przepisami ustawy;
4. jest nieważna na podstawie odrębnych przepisów;
5. jej treść jest niezgodna z warunkami zamówienia;
6. nie została sporządzona lub przekazana w sposób zgodny z wymaganiami technicznymi oraz organizacyjnymi sporządzania lub przekazywania ofert przy użyciu środków komunikacji elektronicznej określonymi przez zamawiającego;
7. została złożona w warunkach czynu nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
8. zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia;
9. została złożona przez wykonawcę niezaproszonego do składania ofert;
10. zawiera błędy w obliczeniu ceny lub kosztu;
11. wykonawca w wyznaczonym terminie zakwestionował poprawienie omyłki, o której mowa w art. 223 ust. 2 pkt 3;
12. wykonawca nie wyraził pisemnej zgody na przedłużenie terminu związania ofertą;
13. wykonawca nie wyraził pisemnej zgody na wybór jego oferty po upływie terminu związania ofertą;
14. wykonawca nie wniósł wadium, lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 – w przypadku gdy zamawiający wymagał jego wniesienia;
15. oferta wariantowa nie została złożona lub nie spełnia minimalnych wymagań określonych przez zamawiającego, w przypadku gdy zamawiający wymagał jej złożenia;
16. jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;
17. obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe;

18. została złożona bez odbycia wizji lokalnej lub bez sprawdzenia dokumentów niezbędnych do realizacji zamówienia dostępnych na miejscu u zamawiającego, w przypadku gdy zamawiający tego wymagał w dokumentach zamówienia.

XX. Wybór wykonawcy i zawarcie umowy

Wybór wykonawcy:

Zamawiający podpisze umowę z wykonawcą, który:

1. Złożył ofertę odpowiadającą wymaganiom określonym w niniejszej specyfikacji,
2. Przedłożył ofertę najkorzystniejszą z punktu widzenia kryteriów przyjętych w niniejszym postępowaniu.

Ogłoszenie wyników postępowania:

1. Postępowanie o udzielenie zamówienia publicznego kończy się zawarciem umowy lub jego unieważnieniem.
2. Zamawiający **unieważni postępowanie**, jeśli zaistnieje którakolwiek z obligatoryjnych przesłanek, przewidzianych w art. 255 pzp.
3. Jeśli nie zaistnieją przesłanki unieważnienia postępowania, Zamawiający dokona wyboru najkorzystniejszej oferty.
4. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zawiadamia Wykonawców, którzy złożyli oferty, o:
    a) wyborze najkorzystniejszej oferty, podając nazwę (firmę), siedzibę i adres Wykonawcy, którego ofertę wybrano oraz uzasadnienie jej wyboru, a także nazwy (firmy), siedziby i adresy Wykonawców, którzy złożyli oferty wraz ze streszczeniem oceny i porównania złożonych ofert zawierającym punktacje przyznaną ofertom w każdym kryterium oceny ofert i łączną punktacje;
    b) Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne;
    c) Wykonawcach, którzy zostali wykluczeni z postępowania o udzielenie zamówienia podając uzasadnienie faktyczne i prawne;

Zawarcie umowy:

Zamawiający zawiera umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przekazania zawiadomienia o wyborze oferty.

XXI. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawartej umowy w sprawie zamówienia publicznego.

Projekt istotnych postanowień umowy stanowi załącznik nr 9.

XXII. Środki ochrony prawnej

1. Środki ochrony prawnej przysługują Wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy.

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, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
   - niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy
   - zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy;
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej.
5. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy Pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
6. Szczegółowe informacje dotyczące środków ochrony prawnej (zasady, terminy oraz sposób korzystania ze środków ochrony prawnej) określone są w Dziale IX „Środki ochrony prawnej" ustawy Pzp.9at 505-590)

XXIII KLAUZULA INFORMACYJNA Z ART. 13 RODO

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 119z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1. administratorem Pani/Pana danych osobowych jest **Zespół Opieki Zdrowotnej we Włoszczowie - Szpital Powiatowy im. Jana Pawła II, ul. Żeromskiego 28, 29-100 Włoszczowa, tel.(41)3883765, e-mail: dane.osobowe@zozwloszczowa.pl***;*
   Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b i c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. **„Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Zespole Opieki Zdrowotnej we Włoszczowie – Szpitalu Powiatowym im. Jana Pawła II", Znak sprawy: 09/09/2023**, prowadzonym w trybie podstawowym bez negocjacji na podstawie art. 275 pkt 1;
2. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy z dnia 11 września 2019r. Prawo Zamówień Publicznych (Dz. U. z 2019r, poz. 2019 ze zm., dalej - ustawa PZP);
3. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 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;
4. 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;
5. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
6. posiada Pani/Pan:
   1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   2. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;

3. 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 ***;
4. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
5. 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.

*** Wyjaśnienie:** informacja w tym zakresie jest wymagana, jeżeli w odniesieniu do danego administratora lub podmiotu przetwarzającego istnieje obowiązek wyznaczenia inspektora ochrony danych osobowych.
**** Wyjaśnienie:** 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.
***** Wyjaśnienie:** 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.

Załączniki do SWZ:
Specyfikacja Warunków Zamówienia wraz z załącznikami:
Załącznik nr 1 – szczegółowy opis przedmiotu zamówienia;
Załącznik nr 2 - formularz ofertowy;
Załącznik nr 3 (a i b) - oświadczenie o spełnieniu warunków udziału w postępowaniu;
Załącznik nr 4 (a i b) – oświadczenie o braku podstaw do wykluczenia;
Załącznik nr 5 – wzór wykazu dostaw/usług;
Załącznik nr 6 – oświadczenie Grupa Kapitałowa – wzór;
Załącznik nr 7 – oświadczenie dot. aktualności informacji;
Załącznik nr 8 – oświadczenie wykonawców;
Załącznik nr 9 – istotne postanowienia umowy.

Zatwierdził

Szczegółowy Opis Przedmiotu Zamówienia

PAKIET NR 1

1. System kopii zapasowych

Sprzętowe		
Wymagane minimalne parametry techniczne		**Tak, podać**
Obudowa	Obudowa Rack o wysokości max 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
Procesor	Zainstalowany jeden procesor 8-rdzeniowy, min. 2.8 GHz (Turbo Speed min. 3.6 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 19220 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.	
RAM	32GB DDR4 RDIMM	
Interfejsy sieciowe/FC/SAS	min. 2szt. Ethernet 1Gb, Dual SFP+	
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 2 dyski SSD o pojemności min. 480GB Urządzenie powinno posiadać już zainstalowane dyski oraz skonfigurowany RAID 5 lub 6 i być gotowe do pracy	
Zasilacze	Redundantne, min. 600W każdy	
Warunki gwarancji	NBD on-premise: Analogicznie do czasu trwania supportu oprogramowania	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.	
Wsparcie techniczne	• Pomoc techniczna w językach: ○ polskim, ○ angielskim. • Świadczone jest bezpośrednio przez główną siedzibę	

	producenta. • Zapewnia dostęp do aktualizacji oprogramowania, • Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, • Obowiązuje przez okres minimum 60 miesięcy.	
Ogólne		
System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.		
Konsola zarządzająca może być również instalowana w chmurze producenta zlokalizowanej na terenie Polski		
Interfejs systemu dostępny jest w języku: • polskim, • angielskim		
System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, w tym z możliwością odtworzenia w postaci usługi uruchomionej w chmurze producenta zlokalizowanej na terenie Polski		
Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej)		
Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych		
Zarządzanie		
Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli, dostępnej za pośrednictwem przeglądarki WWW		
Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego		
Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem		
Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym		

harmonogramem	
Monitorowanie postępu działania zadania	
Posiada system powiadamiania poprzez e-mail bądź Slack o zdarzeniach w następujących przypadkach: • Zadanie zostało zakończone pomyślnie • Zadanie zostało zakończone z ostrzeżeniami, • Zadanie zostało zakończone z błędem • Zadanie zostało anulowane • Zadanie nie zostało uruchomione	
System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego	
System umożliwia wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika	
Możliwość zdefiniowania okna backupowego dla każdego z zadań	
Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów i innych sekretów, wykorzystywanych przez System	
System pozwala na klonowanie planów kopii zapasowych	
System umożliwia reset hasła administratora w przypadku jego utraty	
Oprogramowanie umożliwia definiowanie retencji według schematów: • GFS(Grandfather-Father-Son) • FIFO(First-In, First-Out)	
Oprogramowanie umożliwia tworzenie grup urządzeń	
Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do	

przeszukiwania m.in. magazynów)	
System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: • System Administrator • Backup operator • Restore operator • Viewer	
Składowanie danych	
Dane są składowane w ramach dostępnej macierzy wymienionej w wymaganiach sprzętowych OPZ	
System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle	
System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami	
System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych	
System obsługuje mechanizm WORM (Write Once Ready Many) w chmurowych oraz lokalnych repozytoriów kopii	
Odtwarzanie	
Odtwarzanie granularne: • Pojedynczych plików z kopii obrazu dysku, • Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365	
Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: • Windows: 7+ • Windows Server: 2008 R2+	
Odtwarzanie Bare Metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników	

przez użytkownika	
Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a	
Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V	
Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(RAW, VHD, VHDX, VMDK)	
Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL)	
Odtwarzanie zasobów plikowych z prawami dostępu	
Przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows)	
Odtwarzanie danych według harmonogramu	
Przywracanie danych z określonego urządzenia/użytkownika	
Przywracanie kopii z wybranego magazynu	
Przywracanie danych Microsoft 365: • do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst • do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)	
System posiada możliwość nieodwracalnego kasowania danych	
Przywracanie repozytoriów GIT: • Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket/GitLab), • przywracanie między kontami.	
Backup	
Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych dla:	

- Systemów operacyjnych:
    - Alpine 3.10+
    - Debian: 9+
    - Ubuntu: 16.04+
    - Fedora: 29+
    - centOS: 7+
    - RHEL: 6+,
    - openSUSE: 15+
    - SUSE Enterprise Linux(SLES): 12 SP2+
    - macOS: 10.13+
    - Windows: 7 i nowsze
    - Windows Server: 2008 R2 i nowsze
- Środowisk wirtualnych:
    - Hyper-V
    - VMware

Dowolnych innych – agentowo

Wykonywanie pełnych, różnicowych oraz przyrostowych kopii zapasowych dla:

- Baz danych**:**
    - Microsoft SQL,
    - MySQL,
    - PostgreSQL,
    - Firebird,
    - Oracle

Dowolnych innych przez podpięcie skryptów pre/post.

Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:

• 128 bit • 192 bit • 256 bit	
Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: • ZStandard • LZ4	
Oprogramowanie umożliwia zarządzanie poziomem kompresji	
System dostarcza agenta backupu w postaci kontenera Docker, umożliwiającego wykonywanie kopii zapasowych z dowolnych środowisk kontenerowych, w tym popularnych rozwiązań NAS	
System dostarcza agenta backupu w postaci instalatora MSI, umożliwiającego masową instalację w systemach Windows z wykorzystaniem narzędzi Active Directory - SCCM oraz GPO	
Wykonywanie kopii zapasowej otwartych plików(VSS)	
System umożliwia uruchamianie skryptów przed i po backupie	
System umożliwia uruchamianie skryptów po wykonaniu migawki VSS	
System umożliwia wykonywanie spójnej kopii danych pracujących aplikacji na urządzeniach z systemem Windows oraz wspieranych środowiskach wirtualnych	
System pobiera jedynie zmodyfikowane bloki danych podczas przyrostowej i różnicowej kopii maszyn wirtualnych VMware	
System umożliwia wykonywanie kopii maszyn wirtualnych VMware z zastosowanie zaawansowanych trybów transportu (HotAdd, LAN, SAN), w tym metodą LAN-Free	
System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów	
Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem	

dla partycji MBR oraz GPT	
Backup plikowy	
Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe	
Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia	
Oprogramowanie pozwala na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej	
Oprogramowanie pozwala na backup zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption	
Licencjonowanie	
Licencje powinny pozwalać na zabezpieczenie: • Nielimitowanej ilości maszyn wirtualnych • Nielimitowanej ilości serwerów fizycznych • Nielimitowanej ilości stacji roboczych • Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu	

PAKIET NR 2

2. Oprogramowanie antywirusowe wraz z Endpoint Detection and Response

Wymagane minimalne funkcjonalności
System Operacyjny Windows: **<u>Systemy Operacyjne Komputerów</u>** Pełne wsparcie: • Windows 11 September 2022 Update (22H2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release) • Windows 8.1 • Windows 8 • Windows 7 SP1 **<u>Windows Tablet oraz systemy wbudowane</u>** Pełne wsparcie • Windows 10 IoT Enterprise • Windows Embedded 8.1 Industry • Windows Embedded 8 Standard • Windows Embedded Standard 7 • Windows Embedded Compact 7 • Windows Embedded POSReady 7 • Windows Embedded Enterprise 7

Systemy operacyjne serwera

Pełne wsparcie

- Windows Server 2022 Core
- Windows Server 2022
- Windows Server 2019 Core
- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011

Windows Server 2008 R2

Systemy Operacyjne Linux i wersja kernel

Oparte o RPM

- RHEL 7.x - 3.10.0 (starting from build 957)
- RHEL 8.x - 4.18.0
- RHEL 9x - 5.14.0
- Oracle Linux 7.x (UEK +RHCK) - 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) - 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) – 5.15.0
- CentOS 7.x - 3.10.0 (starting from build 957)
- CentOS 8 Stream- 4.18.0
- CentOS 9 Stream- 5.14.0
- Fedora 31 – 36 - supported until it expires.
- AlmaLinux 8.x - 4.18.0
- AlmaLinux 9.x - 5.14.0
- Rocky Linux 8.x - 4.18.0
- Rocky Linux 9.x - 5.14.0
- CloudLinux 8.x - 4.18.0
- CloudLinux 7.x - 3.10
- Miracle 8.4 - 4.18.0

Oparte o Debian

- Debian 9 - 4.9.0
- Debian 10 - 4.19
- Debian 11 - 5.10
- Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15
- Ubuntu 18.04.x - 5.0 / 5.3 / 5.4

- Ubuntu 20.04.x - 5.4
- Ubuntu 21.10.x - 5.13
- Ubuntu 22.04.x - 5.15
- PopOS 22.04.x – 6.2
- Pardus 21 – 5.10
- Mint 20.3 – 5.4.0
- Mint 21 – 5.15.0

Oparte o SUSE

- SLES 12 SP4 - 4.12.14-x
- SLES 12 SP5 - 4.12.14-x
- SLES 15 SP1 - 4.12.14-x
- SLES 15 SP2 - 5.3.18-x
- SLES 15 SP3 - 5.3.18-x
- SLES 15 SP4 – 5.14.21
- openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x

- Cloud based Linux
- AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x
- Amazon Linux v2 - 4.14.x / 4.19.x, 5.10
- Amazon Linux 2023 – 6.1.x
- Google COS - -4.19.112 / 5.4.49
- Milestones 77, 81, 85 - 4.19.112 / 5.4.49
- Azure Mariner 2 - 5.15

Systemy Operacyjne Mac OS X

- macOS Ventura (13.x)
- macOS Monterey (12.x)
- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)

Obsługiwane Środowiska Microsoft Exchange

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2019 z rolą Edge Transport lub Mailbox

- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox

Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG).

Ochrona środowisk wirtualnych (SVE)

1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej
2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:
    a) OVA
    b) XVA
    c) VHD
    d) VMDK

Środowiska wspierane:

- VMware vSphere and vCenter Server versions:
    - version 6.5
    - version 6.7, including update 1, update 2a and update 3
    - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2.
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1

- Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition)

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość dodawania wykluczeń na podstawie

a. Plik
b. Folder
c. Rozszerzenie
d. Proces
e. Hash pliku
f. Hash certyfikatu
g. Nazwa zagrożenia
h. Wiersz poleceń
i. IP/maska

13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
20. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH
21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Praca programu musi być niezauważalna dla użytkownika.
29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
32. Możliwość odblokowania ustawień programu po wpisaniu hasła.
33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.

36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
40. Wbudowany IDS
41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.
43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
44. Możliwość tworzenia list sieci zaufanych.
45. Możliwość dezaktywacji funkcji zapory sieciowej.
46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa)
50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
52. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
    a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

       -Ochrony przeglądarki internetowej
       -Sieć i poświadczenia
       -Błędna konfiguracja systemu operacyjnego
       System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.
    b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy

tym numer CVE tych luk.

c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f)System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

a) Możliwość wymuszenia funkcji DEP systemu Windows

b) Możliwość wymuszenia relokacji modułów (ASLR)

<u>Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.</u>

54. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:

-Wczesny dostęp
-Dostęp do poświadczeń
-Wykrycie
-Crimeware

55. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

Formaty plików jakie mogą być odzyskane:
3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:

a) Ukierunkowane ataki

b) Podejrzane pliki i ruch w sieci

c) Exploity

d) Ransomware

e) Grayware

57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego

58. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:

a) Tolerancyjny

b) Normalny

c) Agresywny

59. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku

a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora

b) Możliwość przesłania archiwum zabezpieczonego hasłem

c) Możliwość przesłania adresu URL

d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.

60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania

61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny

62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.

63. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.

64. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB

65. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.

66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).

67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem.
4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

Stacje robocze i serwery Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów

14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Ochrona Exchange

3. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
4. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.
5. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
6. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.
7. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.
8. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
9. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
10. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
11. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
12. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.

13. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.

14. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3. Możliwość integracji wielu domen Active Directory
4. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
9. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
10. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
11. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
12. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
13. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
14. Możliwość generowania raportu co godzinę.
15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
16. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
17. Możliwość dodania etykiety do stacji roboczej.
18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji

zdalnej.

19. Możliwość przechowywania kwarantanny maksymalnie 180 dni
20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
21. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
22. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
23. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[2]
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie

    -Zakres adresów IP/IP
    -Adres bramy
    -Adres serwera WINS
    -Adres serwera DNS
    -Połączenie DHCP sufiksów DNS
    -Punkt końcowy może rozwiązać hosta
    -Typ sieci
    -Nazwa hosta
27. Integracja z serwerem Syslog.
28. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238
29. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
30. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
31. Funkcja pojedynczego logowania – Single Sign-on (SSO).
32. Możliwość naprawy instalacji z poziomu konsoli.
33. Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

    -Zarządzane punkty końcowe
    -Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
    -Pięć najczęściej blokowanych zagrożeń
    -Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
    -Status incydentów bezpieczeństwa które wystąpiły
    -Stan modułów punktów końcowych
    -Ocena ryzyka firmy
    -Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie,

phishing, oszustwa.
-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

34. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Pakiety
    b) Sieć
    c) Kwarantanna
    d) Licencjonowanie
    e) Integracje
    f) Polityki
    g) Raporty
    h) Konta
    i) Firmy
35. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane
36. Możliwość określenia własnego serwera NTP.
37. Integracja z vCenter Server.
38. Integracja z Xen Server.
39. Integracja z nutanix Prism Element.
40. Możliwość integracji z Amazon EC2.
41. Intergracja z Azure.
42. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
43. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
44. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
45. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:
    a) Lotnictwo
    b) Rolnictwo
    c) Automotive

d) Usługi komercyjne

e) Doradztwo

f) Energia

g) Usługi finansowe

h) Rząd

i) Opieka zdrowotna

j) Technologie

k) Transport

l) Non-profit

m) Górnictwo

n) Media

46. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
47. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.
48. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
49. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
50. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
51. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
52. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
53. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
54. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
55. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
56. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
57. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
58. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do

darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

59. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
60. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.

Wspierane systemy operacyjne

A. Systemy desktopowe

- Windows 11 (initial)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial)
- Windows 8.1
- Windows 8
- Windows 7 SP1

B. Systemy operacyjne dla serwerów:

- Windows Server 2022

- Windows Server 2019 Core
- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

C. MacOS:

- macOS Monterey (12.x)
- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)

D. Linux

- Oparte o RPM
- RHEL 7.x - 3.10.0 (starting from build 957)
- RHEL 8.x - 4.18.0
- RHEL 9x - 5.14.0
- Oracle Linux 7.x (UEK +RHCK) - 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) - 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) – 5.15.0
- CentOS 7.x - 3.10.0 (starting from build 957)
- CentOS 8 Stream- 4.18.0
- CentOS 9 Stream- 5.14.0
- Fedora 31 – 36 - supported until it expires.
- AlmaLinux 8.x - 4.18.0
- AlmaLinux 9.x - 5.14.0
- Rocky Linux 8.x - 4.18.0
- Rocky Linux 9.x - 5.14.0
- CloudLinux 8.x - 4.18.0
- CloudLinux 7.x - 3.10
- Miracle 8.4 - 4.18.0

Oparte o Debian

- Debian 9 - 4.9.0
- Debian 10 - 4.19
- Debian 11 - 5.10
- Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15
- Ubuntu 18.04.x - 5.0 / 5.3 / 5.4
- Ubuntu 20.04.x - 5.4
- Ubuntu 21.10.x - 5.13
- Ubuntu 22.04.x - 5.15
- PopOS 22.04.x – 6.2
- Pardus 21 – 5.10
- Mint 20.3 – 5.4.0
- Mint 21 – 5.15.0

Oparte o SUSE

- SLES 12 SP4 - 4.12.14-x
- SLES 12 SP5 - 4.12.14-x
- SLES 15 SP1 - 4.12.14-x
- SLES 15 SP2 - 5.3.18-x
- SLES 15 SP3 - 5.3.18-x
- SLES 15 SP4 – 5.14.21
- openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x

- Cloud based Linux
- AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x
- Amazon Linux v2 - 4.14.x / 4.19.x, 5.10
- Amazon Linux 2023 – 6.1.x
- Google COS - -4.19.112 / 5.4.49
- Milestones 77, 81, 85 - 4.19.112 / 5.4.49
- Azure Mariner 2 - 5.15

Komponenty EDR

Główne elementy:

1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i

ruchu sieciowego oraz filtr stron internetowych.

Wykrywanie podejrzanej aktywności

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.

1. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
2. Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
2. Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:

a) Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.

b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.

c) Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

Incydenty

Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

a) Filtrowania zdarzeń

b) Blokowania procesów

c) Dodawanie procesów do czarnej listy

d) Dodawanie procesów do białej listy

e) Izolacja hosta

f) Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)

g) Przesłanie pliku do Sandbox

h) Sprawdzenie informacji o pliku w Google

i) Sprawdzenie informacji o pliku w VirusTotal

Filtrowanie zdarzeń odbywa się na podstawie:

a) Ocena zagrożenia od 10 do 100 punktów

b) Data wykrycia

c) Status

d) ID

e) Nazwa punktu końcowego

f) Typ ataku

a) Ransomware

b) Potencjalnie niechciana aplikacja

c) Malware

d) Exploit

e) Fileless

f) Password stealer

g) Downloader

h) Inne

i) Zdefiniowane przez użytkownika

Wyszukiwanie zdarzeń może odbywać się na podstawie:

a) Nazwa alertu

b) IP punktu końcowego

c) Hash MD5

d) Hash SHA256

e) Nazwa użytkownika

Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem.

Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.

Możliwość wyświetlenia zablokowanych hashy plików.

Możliwość dodania własnych hashy MD5 oraz SHA256

Możliwość importu hashy z pliku CSV

Możliwość filtrowania dodanych hashy na podstawie:

a) Typu hashu

b) Wartości hash

c) Źródło dodania

d) Informacje o źródle

e) Nazwa pliku

f) Firma której dotyczy wpis

g) Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.

Konsola Cloud – serwer administracyjny po stronie producenta

1. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).

2. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:

a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

-Ochrony przeglądarki internetowej

-Sieć i poświadczenia

-Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie.

3. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

a) Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.

b) Funkcja pojedynczego logowania – Single Sign-on (SSO).

c) Możliwość naprawy instalacji z poziomu konsoli.

d) Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

-Zarządzane punkty końcowe

-Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne

-Pięć najczęściej blokowanych zagrożeń

-Podział zagrożeń na urządzenia takie jak stacje robocze i serwery

-Status incydentów bezpieczeństwa które wystąpiły

-Stan modułów punktów końcowych

-Ocena ryzyka firmy

-Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.

4. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

a) Lotnictwo

b) Rolnictwo

c) Automotive

d) Usługi komercyjne

e) Doradztwo

f) Energia

g) Usługi finansowe

h) Rząd

i) Opieka zdrowotna

j) Technologie

k) Transport

l) Non-profit

m) Górnictwo

n) Media

5. Możliwość integracji sekcji Firmy z innymi systemami poprzez API.

6. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i

innych.

8. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

9. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:

a) historia powłoki

b) wczytywanie bibliotek .dll z podejrzanej lokalizacji

c) Sesje logowania z użyciem jawnych danych uwierzytelniających

d) Elementy startowe Windows

e) Arp cache

f) Ip forwarding

g) Pobieranie listy wszystkie otwarte pliki dla każdego procesu w systemie docelowym.

h) Lista zamontowanych nośników

i) Filtry ip tables

j) Połączenia TLS które używają certyfikatów self-signed

k) Używane rozszerzenia w przeglądarce Chrome

l) Używane rozszerzenia w przeglądarce Firefox

m) Używane rozszerzenia w przeglądarce Safari

n) Źródła apt w systemach Linux

o) Wyświetlanie zainstalowanych pakietów DEB

p) Wyświetlanie zainstalowanych pakietów RPM

q) Pakiety Python zainstalowane w systemie

r) Lista zainstalowanych użytkowników którzy łączyli się z publicznych adresów IP

s) Lista użytkowników którzy zostali utworzeni w ciągu ostatnich 30 dni(Linux)

t) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS

u) Wykrywanie czy Kontrola Kont Użytkowników(UAC) jest wyłączona

v) Wykrywanie czy SecureBoot jest włączony

w) Lista zapamiętanych połączeń bezprzewodowych

x) Wykrywa, czy zmienił się domyślny folder startowy użytkownika

y) Wykrywa, czy zmienił się domyślny folder startowy maszyny

Załącznik nr 2 do SWZ

FORMULARZ OFERTOWY

1. **Dane dotyczące oferenta:**

Nazwa .....

Siedziba .....

Tel. / fax. .....

NIP .....

REGON .....

E-mail ……

2. Zobowiązuję się zrealizować przedmiot zamówienia za łączną kwotę:

a) **Pakiet nr 1 Netto: ....., VAT: ....., Brutto: .....**

(słownie brutto: ..... złotych).

b) **Pakiet nr 2 Netto: ....., VAT: ....., Brutto: .....**

(słownie brutto: ..... złotych).

3. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i przyjmujemy je bez zastrzeżeń.
4. Oświadczamy, że akceptujemy zawarty w Specyfikacji Warunków Zamówienia projekt umowy i zobowiązujemy się do jej podpisania w przypadku wyboru naszej oferty.
5. Oświadczamy, że przedmiot zamówienia zrealizujemy w terminie:
   a) **Pakiet nr 1: .....** dni od podpisania Umowy**,**
   b) **Pakiet nr 2: .....** dni od podpisania Umowy.
6. Z naszej strony realizację zamówienia koordynować będzie: …… tel. ……, e-mail…….
7. Oferta zawiera/nie zawiera * informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji.
8. Oświadczamy, iż wybranie naszej oferty jako najkorzystniejszej **nie wiąże/wiąże*** się dla Zamawiającego z poniesieniem żadnych dodatkowych kosztów podwyższających cenę oferty, w szczególności wynikających z powstania obowiązku podatkowego, po stronie Zamawiającego ……

9. Oświadczam, że firma, którą reprezentuję jest: mikroprzedsiębiorstwem*****, małym przedsiębiorstwem *****, średnim przedsiębiorstwem***** dużym przedsiębiorstwem*.
10. Oświadczam, że zamierzam/nie zamierzam* powierzyć następującej części zamówienia …… podwykonawcom……..
11. W razie wybrania naszej oferty zobowiązujemy się do podpisania umowy na warunkach zawartych w dokumentacji oraz w miejscu i terminie określonym przez Zamawiającego. Osobami uprawnionymi do reprezentowania firmy, które będą podpisywać umowę są:

…… ……

stanowisko imię i nazwisko

12. Oświadczenie Wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub 14 RODO:

*„Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu." ****

***** 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 – przekreśla treść oświadczenia.**

**** - niepotrzebne skreślić***

.....

imię i nazwisko podpis uprawnionego
przedstawiciela oferenta

Załącznik nr 3 a do SWZ

Zamawiający:

Zespół Opieki Zdrowotnej we Włoszczowie
ul. Żeromskiego 28
29-100 Włoszczowa

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako ustawa Pzp)

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II, Znak sprawy: 09/09/2023”** oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w **SWZ.**

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w **pkt …….. SWZ,** polegam na zasobach następującego/ych podmiotu/ów:

……

……..,

w następującym zakresie:

……

…… *(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).*

Uwaga: W przypadku gdy Wykonawca nie powołuje się na zasoby podmiotów trzecich w przedmiotowym postepowaniu oświadczenie należy wykreślić. Zamawiający równoznacznie ze skreśleniem oświadczenia będzie rozumiał nie uzupełnienie jego treści.

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.

……

Załącznik nr 3 b do SWZ

Zamawiający:

Zespół Opieki Zdrowotnej we Włoszczowie
ul. Żeromskiego 28
29-100 Włoszczowa

Wykonawca

……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy udostępniającego zasoby

składane na podstawie art. 125 ust. 5 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako ustawa Pzp)

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II, Znak sprawy: 09/09/2023”,** oświadczam, co następuje:
Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w **SWZ,** w następującym zakresie **tj. dotyczy warunku udziału określonego w pkt …… SWZ**

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.

……

Załącznik nr 4 a do SWZ

Zamawiający:

Zespół Opieki Zdrowotnej we Włoszczowie
ul. Żeromskiego 28
29-100 Włoszczowa

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako ustawa Pzp)

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II, Znak sprawy: 09/09/2023”**, oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

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

   Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ustawy Pzp. w zakresie określonym przez Zamawiającego w SWZ.

2. Oświadczam, że **zachodzą** w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 6 lub 109 ust 1 pkt 2-5, 7-10, ustawy Pzp.).* Jednocześnie oświadczam,

   że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp. podjąłem następujące środki naprawcze:

   ……

   ……

Uwaga: W przypadku gdy nie zachodzą w stosunku do Wykonawcy okoliczności o których mowa w oświadczenia należy wykreślić treść oświadczenia. Zamawiający równoznacznie ze skreśleniem oświadczenia będzie rozumiał nie uzupełnienie jego treści

Jednocześnie oświadczam, iż wobec wykonawcy, którego reprezentuję brak jest podstaw do wykluczenia o których mowa w 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.

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.

……

Załącznik nr 4 b do SWZ

Zamawiający:

Zespół Opieki Zdrowotnej we Włoszczowie
ul. Żeromskiego 28
29-100 Włoszczowa

Wykonawca:

……

……

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie podmiotu udostepniającego zasoby

składane na podstawie art. 125 ust. 5 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako ustawa Pzp)

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II, Znak sprawy: 09/09/2023”**, oświadczam, co następuje:

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

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ustawy Pzp. w zakresie określonym przez Zamawiającego w SWZ.

2. Oświadczam, że **zachodzą** w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 6 lub 109 ust 1 pkt 2-5, 7-10, ustawy Pzp.).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 u.p.z.p. podjąłem następujące środki naprawcze:
.....
.....
.....

Uwaga: W przypadku gdy nie zachodzą w stosunku do Wykonawcy okoliczności o których mowa w oświadczenia należy wykreślić treść oświadczenia. Zamawiający równoznacznie ze skreśleniem oświadczenia będzie rozumiał nieuzupełnienie jego treści

Jednocześnie oświadczam, iż wobec wykonawcy, którego reprezentuję brak jest podstaw do wykluczenia o których mowa w 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.

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.

…….

(pieczęć adresowa firmy Wykonawcy)

WYKAZ WYKONANYCH LUB WYKONYWANYCH W CIĄGU OSTATNICH TRZECH LAT DOSTAW/USŁUG

Niniejszym oświadczam, że w okresie ostatnich 3 lat, podmiot, który reprezentuję w niniejszym postępowaniu zrealizował/realizuje wymienione w tabeli dostawy/usługi, polegające na dostarczeniu licencji i wdrożeniu systemu kopii zapasowych o wartości minimum 200 000,00 brutto.

Wymagane informacje należy podać za okres ostatnich 3 lat, a w przypadku, gdy okres prowadzenia działalności jest krótszy – za ten okres.

Lp.	Nazwa Zamawiającego u którego wykonano lub wykonuje się zamówienie	Adres Zamawiającego	Terminy realizacji zamówienia	Wartość zamówienia brutto

W załączeniu dokumenty / referencje / potwierdzające należyte wykonanie/wykonywanie wyszczególnionych wyżej zamówień

Miejsce i data .....

.....
Podpisy i pieczątki imienne przedstawicieli Wykonawcy upoważnionych do jego reprezentowania

Załącznik nr 6 do SWZ

„Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej”

W związku z udziałem w postępowaniu pn. **„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II, Znak sprawy: 09/09/2023”** jako **Wykonawca/ Podmiot udostępniający zasoby*** ubiegający się o udzielenie zamówienia ……. *(nazwa Wykonawcy)* oświadczam, że:

1) nie przynależę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2020 r. poz. 1076 i 1086), z innym Wykonawcą, który złożył odrębną ofertę;[1]

2) przynależę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2020 r. poz. 1076 i 1086) z następującym Wykonawcą, który złożył odrębną ofertę, tj.:[1]

   ……

   ……

   (nazwa i adres Wykonawcy, który przynależy do tej samej grupy kapitałowej i złożył odrębną ofertę)

   Jednocześnie w celu wykazania braku podstawy wykluczenia składam dokumenty/informacje potwierdzające przygotowanie oferty niezależnie od Wykonawcy wskazanego w pkt 2 powyżej.[2]

[1] niepotrzebne skreślić lub usunąć

[2] w przypadku złożenia oświadczenia w pkt 2 należy przedłożyć wraz z niniejszym oświadczeniem dokumenty lub przedstawić informacje potwierdzające przygotowanie oferty niezależnie od Wykonawcy przynależącego do tej samej grupy kapitałowej

Załącznik nr 7 do SWZ

Zamawiający:

Zespół Opieki Zdrowotnej we Włoszczowie
ul. Żeromskiego 28
29-100 Włoszczowa

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:

……
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy/ Podmiotu udostępniającego zasoby*

o aktualności informacji zawartych w oświadczeniu,

o którym mowa w art. 125 ust 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako ustawa Pzp.),

w zakresie podstaw wykluczenia z postepowania określonych w SWZ

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych dla Zespołu Opieki Zdrowotnej we Włoszczowie – Szpitala Powiatowego im. Jana Pawła II, Znak sprawy: 09/09/2023”** prowadzonego przez Zespół Opieki Zdrowotnej we Włoszczowie – Szpital Powiatowy im. Jana Pawła II, oświadczam, co następuje:

Oświadczam, że informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust 1 ustawy Pzp. w zakresie podstaw wykluczenia z postepowania określonych w SWZ o których mowa:

- w art. 108 ust 1 pkt 1, 3, 4, 5, 6 ustawy Pzp.,
- w art. 109 ust 1 pkt 1 ustawy Pzp.

pozostają aktualne oraz są zgodne z prawdą i zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu tych informacji.

Jednocześnie oświadczam, iż wobec wykonawcy, którego reprezentuję w dalszym ciągu brak jest podstaw do wykluczenia o których mowa w 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.

* Niepotrzebne skreślić

Załącznik nr 8 do SWZ

„Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia"

Jako Wykonawcy wspólnie ubiegający się o udzielenie zamówienia:

1) …….. (nazwa i adres Wykonawcy)
2) …….. (nazwa i adres Wykonawcy)
3) …….. (nazwa i adres Wykonawcy)

w postępowaniu pn. **……..** oświadczamy, że:

1) warunek udziału w postępowaniu, o którym mowa w rozdziale XI.I ust. 1 lit d SWZ spełnia:

……

……..

(wskazanie danych Wykonawcy spełniającego warunek)

Oświadczamy, że wskazany powyżej Wykonawca wykona dostawy/usługi, do których spełnienie warunków, o których mowa w rozdziale XI.I ust. 1 lit d SWZ jest wymagane, tj. zakres przedmiotowy określony w przedmiocie zamówienia.

Załącznik nr 9 do SWZ

UMOWA NR …./…. /2023

NA DOSTAWĘ OPROGRAMOWANIA I SPRZĘTU PODNOSZĄCEGO POZIOM CYBERBEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH DLA ZESPOŁU OPIEKI ZDROWOTNEJ WE WŁOSZCZOWIE – SZPITALA POWIATOWEGO IM. JANA PAWŁA II

zawarta we Włoszczowie w dniu ……2023 roku pomiędzy:

1. **Zespołem Opieki Zdrowotnej we Włoszczowie - Szpitalem Powiatowym im. Jana Pawła II**, ul. Żeromskiego 28, 29-100 Włoszczowa; wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym w Kielcach, X Wydział Gospodarczy KRS pod numerem KRS: 0000057160, NIP 6561855908, REGON 000304295, reprezentowanym przez:
……..,
przy kontrasygnacie……..,
zwanym dalej „**Zamawiającym**”,
a
2. ……
……
reprezentowaną przez:
zwaną dalej „**Wykonawcą**”,
……
zwanymi dalej łącznie „Stronami”, a osobno „Stroną”,
o następującej treści:

Niniejsza Umowa została zawarta w wyniku rozstrzygnięcia trybu podstawowego bez negocjacji na podstawie art. 275 pkt 1, przeprowadzonego na podstawie przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz.U. z 2023 r., poz. 1605.)
Strony Umowy w wyniku tego rozstrzygnięcia ustalają, co następuje.

§ 1

Przedmiot Umowy

1. Przedmiotem Umowy jest dostawa **oprogramowania i sprzętu określonego w pakiecie nr …….** .
2. Opis parametrów oprogramowania i sprzętu zawiera Szczegółowy Opis Przedmiotu Zamówienia stanowiący Załącznik nr 1 do Umowy.

§2

Oświadczenia i zapewnienia Stron

1. Wykonawca oświadcza, że posiada prawo świadczenia usług objętych Umową oraz że jest uprawniony do wprowadzania oprogramowania do obrotu i używania na terenie Polski, oraz że uprawnienie to nie wygasło, ani nie zostało odwołane, zbyte ani ograniczone.

2. Wykonawca oświadcza, że objęte niniejszą Umową oprogramowanie i sprzęt pochodzić będzie z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.
3. Wykonawca oświadcza, że dostarczane oprogramowanie i sprzęt są fabrycznie nowe, nieużywane, wolne od wad fizycznych i prawnych i nie są przedmiotem praw lub roszczeń osób trzecich.
4. Wykonawca dostarczy wszelkie dokumenty dotyczące sprzętu, w szczególności dokumenty niezbędne do jego prawidłowej eksploatacji, sporządzone w języku polskim, w tym w szczególności instrukcję obsługi sprzętu oraz dokumenty gwarancyjne sprzętu potwierdzające fakt uzyskania przez Zamawiającego uprawnień gwarancyjnych (o ile dotyczy).
5. Strony deklarują współpracę w celu realizacji przedmiotu Umowy. W szczególności Strony zobowiązane są do wzajemnego powiadamiania się o ważnych okolicznościach mających lub mogących mieć wpływ na wykonanie przedmiotu Umowy, w tym na ewentualne opóźnienia.
6. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury oraz pomieszczeń niezbędnych do realizacji Umowy.
7. Zamawiający oświadcza, że jest świadomy konsekwencji braku dokonywania i weryfikacji poprawności kopii bezpieczeństwa danych i systemów, jak również nienależytego zabezpieczenia nośników i infrastruktury. Zamawiający zobowiązuje się do wykonania kopii bezpieczeństwa swoich systemów i weryfikacji jej poprawności przed przystąpieniem przez Wykonawcę do realizacji prac wdrożeniowych z oprogramowaniem stanowiącym przedmiot Umowy .
8. Wykonawca nie ponosi odpowiedzialności za szkody wywołane którąkolwiek z następujących okoliczności, a w wypadku ich wystąpienia Zamawiający zobowiązuje się przekazać Wykonawcy poprawną kopię danych, o której mowa w ust. powyżej w celu naprawienia szkody:
   a) utrata danych,
   b) brak możliwości odtworzenia utraconych danych,
   c) utrudnienie w korzystaniu lub całkowita utrata możliwości eksploatacji, oprogramowania lub innych programów, jeżeli jest spowodowana utratą danych,
   d) zaniechanie Zamawiającego, w należytym zabezpieczaniu Infrastruktury,
   e) szkody będące następstwami okoliczności wymienionych powyżej lub wynikające z powodu okoliczności za które wyłącznej odpowiedzialności nie ponosi Wykonawca.

§ 3

Osoby upoważnione do kontaktu

1. Osobą upoważnioną do kontaktów oraz odbioru przedmiotu Umowy ze Strony Zamawiającego jest:
   imię, nazwisko: **……**.
   numer telefonu: **……, *email:* ……**
2. Osobą upoważnioną ze strony Wykonawcy jest:
   imię, nazwisko: **……**
   numer telefonu: **……, *email:* ……**
3. Strona poinformuje drugą stronę niniejszej Umowy, na piśmie pod rygorem nieważności,

o każdorazowej zmianie osoby uprawnionej do kontaktów, zmianie jej danych, a w szczególności zmianie numerów telefonów.

§4

Zasady dostawy i wdrożenia

1. Dostawa i wdrożenie przedmiotu Umowy nastąpi na koszt i ryzyko Wykonawcy. Dostawa nastąpi dowolnym środkiem transportu do siedziby Zamawiającego – Miejsca Dostawy.
2. Wykonawca dostarczy przedmiot Umowy do Miejsca Dostawy i rozmieści/zainstaluje je w miejscach wskazanych przez Zamawiającego.
3. Wykonawca oświadcza, że zapoznał się z warunkami i możliwościami dostawy oraz rozmieszczenia lub instalacji przedmiotu Umowy w Miejscu Dostawy.
4. Strony akceptują fakt, że usługi wdrożeniowe, szkoleniowe i serwisowe mogą być wykonywane poza siedzibą Zamawiającego lub zdalnie.
5. Zamawiający zapewni Wykonawcy możliwość instalacji urządzeń lub oprogramowania narzędziowego, umożliwiających zdalny, bezpieczny szyfrowany dostęp do infrastruktury, w szczególności serwera/ów, na którym/ch posadowione jest oprogramowanie Zamawiającego z którym oprogramowanie stanowiące przedmiot Umowy będzie w interakcji.

§ 5

Termin i odbiór przedmiotu Umowy

1. Wykonawca zobowiązany jest do realizacji przedmiotu Umowy w terminie do …… .
2. Wykonanie przedmiotu niniejszej Umowy będzie potwierdzone protokołem odbioru końcowego podpisanym przez Zamawiającego i Wykonawcę.
3. O gotowości do odbioru przedmiotu Umowy Wykonawca powiadomi Zamawiającego, który w terminie do 5 dni od powiadomienia o gotowości do odbioru przedmiotu Umowy jest zobligowany do podpisania protokołu odbioru całego przedmiotu Umowy, ewentualnie wyspecyfikuje w tym terminie swoje zastrzeżenia co do niezgodności przedmiotu odbioru z przedmiotem Umowy.
4. W przypadku stwierdzenia przez Zamawiającego wad/ uszkodzeń/ zastrzeżeń / braków ilościowych całego przedmiotu niniejszej Umowy Zamawiający sporządzi protokół stwierdzający nieprawidłowości i/lub braki, a Wykonawca zobowiązuje się wymienić przedmiot zamówienia na pełnowartościowy lub uzupełnić braki, w terminie uzgodnionym przez Strony w protokole. W takiej sytuacji Wykonawca powtarza procedurę odbiorową.
5. Dostawa przedmiotu Umowy do Miejsca Dostawy oraz montaż/instalacja/rozmieszczenie/ uruchomienie oraz szkolenie nastąpi w terminie uzgodnionym z Zamawiającym, z zastrzeżeniem § 5 ust.1.
6. Za termin wykonania Umowy rozumie się datę podpisania protokołu końcowego przedmiotu zamówienia bez zastrzeżeń.

§ 6

Wynagrodzenie i warunki płatności

1. Wynagrodzenie za wykonanie Przedmiotu Umowy zostanie wypłacone Wykonawcy po realizacji całego przedmiotu umowy i wynosi: …….. zł netto (słownie: ……..) plus

obowiązująca stawka podatku VAT, to jest łącznie …… zł brutto (słownie: ……..).

2. Ustalone wynagrodzenie jest wynagrodzeniem ryczałtowym, zgodnie ze Specyfikacją Warunków Zamówienia oraz wybraną w trybie postępowania ofertą Wykonawcy, jest niezmienne przez okres realizacji Umowy i obejmuje wszystkie koszty Wykonawcy niezbędne do realizacji niniejszej Umowy zarówno w okresie dostaw, przeszkolenia jak i w okresie udzielonej gwarancji.
3. Płatność nastąpi po odbiorze końcowym wykonania przedmiotu umowy- bez zastrzeżeń, przelewem w terminie do 60 dni od daty doręczenia prawidłowo wystawionej faktury, na rachunek wskazany w jej treści z zastrzeżeniem zastosowania mechanizmu podzielonej płatności polegającym na tym, że:
   a) zapłaty kwoty odpowiadającej całości kwoty podatku wynikającej z otrzymanej faktury jest dokonywana na rachunek VAT;
   b) zapłata całości kwoty odpowiadającej wartości sprzedaży netto wynikającej z otrzymanej faktury jest dokonywana na rachunek bankowy albo na rachunek w spółdzielczej kasie oszczędnościowo-kredytowej, dla których jest prowadzony rachunek VAT, albo jest rozliczana w inny sposób;
   c) podstawą do wystawienia faktury będzie podpisany protokół o którym mowa w § 5 ust. 3.
4. Faktura będzie płatna przelewem na rachunek bankowy wskazany przez Wykonawcę w treści faktury
   w terminie do 60 dni kalendarzowych od daty dostarczenia prawidłowo wystawionej faktury VAT.
5. Za datę zapłaty wynagrodzenia uważa się datę obciążenia rachunku bankowego Zamawiającego.
6. Za ewentualną nieterminową płatność Wykonawca może żądać zapłaty odsetek ustawowych.
7. Wykonawca oświadcza, że rachunek bankowy wskazany na fakturze jest tożsamy z rachunkiem bankowym wskazanym w rejestrze podatników podatku od towarów i usług, z zastrzeżeniem przypadku, gdy Wykonawca będzie zwolniony z podatku od towarów i usług. W przypadku, gdy rachunek wskazany na fakturze nie będzie zgodny z rachunkiem wskazanym w rejestrze podatku od towarów i usług, a Wykonawca nie będzie podlegał zwolnieniu od podatku od towarów i usług, Zamawiający wzywa Wykonawcę do przedłożenia potwierdzenia zmiany rachunku bankowego w przedmiotowym rejestrze w terminie dwóch dni. Jeżeli Wykonawca nie przedstawi dokumentu potwierdzającego zmianę numeru rachunku bankowego w rejestrze podatników podatku od towarów i usług, Zamawiający ma prawo dokonania zapłaty wynagrodzenia na rachunek bankowy wskazany w rejestrze podatników podatku od towarów i usług. W tym wypadku, uznaje się, że Zamawiający prawidłowo wykonał swoje zobowiązanie w zakresie zapłaty wynagrodzenia, a Wykonawcy nie przysługują z tego tytułu żadne roszczenia.
8. Jeżeli Wykonawca nie posiada rachunku bankowego zarejestrowanego w rejestrze podatników podatku od towarów i usług oraz nie przedstawi dokumentu potwierdzającego braku obowiązku rejestracji tegoż rachunku bankowego, Zamawiający ma prawo do wstrzymania zapłaty wynagrodzenia do chwili potwierdzenia rejestracji rachunku bankowego przez Wykonawcę lub przedłożenia dokumentu potwierdzającego brak tegoż obowiązku. Strony zgodnie oświadczają, że wskazane okoliczności nie stanowią opóźnienia lub zwłoki Zamawiającego w zapłacie wynagrodzenia i nie mogą być podstawą jakichkolwiek roszczeń Wykonawcy wobec Zamawiającego.
9. Wykonawca nie ma prawa dokonywać czynności skutkujących bezpośrednim lub pośrednim przeniesieniem wynikających z niniejszej Umowy wierzytelności przysługujących Wykonawcy

w stosunku do Zamawiającego bez jego pisemnej zgody, pod rygorem nieważności, w szczególności Wykonawca nie ma prawa bez zgody Zamawiającego dokonywać przelewu wierzytelności ani ustanawiać ograniczonych praw rzeczowych na wierzytelnościach. Dokonanie ww. czynności bez zgody Zamawiającego będzie skutkować rozwiązaniem Umowy w trybie natychmiastowym i obowiązkiem zapłaty przez Wykonawcę na rzecz Zamawiającego kary umownej w wysokości równowartości przeniesionej/obciążonej wierzytelności.

§ 7

Ochrona danych osobowych i zachowanie poufności

1. Każda ze stron Umowy oświadcza, iż jest Administratorem danych osobowych w rozumieniu 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), zwanego dalej RODO, w odniesieniu do danych osobowych swoich przedstawicieli oraz przedstawicieli drugiej Strony wskazanych w umowie jako osoby do kontaktu (tzw. dane kontaktowe) oraz osoby realizujące przedmiot Umowy. Przekazywane na potrzeby realizacji Umowy dane osobowe są danymi zwykłymi i obejmują w szczególności imię, nazwisko, zajmowane stanowisko i miejsce pracy, numer służbowego telefonu, służbowy adres email.
2. Dane osobowe osób, o których mowa w ust. 1, będą przetwarzane przez Strony na podstawie art. 6 ust. 1 lit. f) RODO (tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratorów danych) jedynie w celu i zakresie niezbędnym do wykonania zadań związanych z realizacją zawartej Umowy.
3. Strony zobowiązują się do ochrony danych osobowych udostępnionych wzajemnie w związku z wykonywaniem Umowy, w tym do wdrożenia oraz stosowania środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa danych osobowych zgodnie z przepisami prawa, a w szczególności z ustawą z dnia 10.05.2018 r. o ochronie danych osobowych oraz przepisami RODO.
4. Strony zobowiązują się poinformować osoby fizyczne niepodpisujące niniejszą Umowę, o których mowa w ust. 1, o treści niniejszego paragrafu.
5. Wykonawca zobowiązuje się do przestrzegania zasad obowiązujących w zakresie ochrony danych osobowych zgodnie z obowiązującymi przepisami prawa – w szczególności w przypadku wdrożenia oraz przeglądów sprzętu w okresie trwania gwarancji, który zawiera dane osobowe.
6. W przypadku powierzenia Wykonawcy przez Zamawiającego do przetwarzania danych osobowych, których Administratorem jest Zamawiający, Strony zobowiązują się do zawarcia Umowy powierzenia przetwarzania danych osobowych.
7. Każda ze Stron jest zobowiązana do zachowania całkowitej poufności wszelkich istotnych informacji odnoszących się do drugiej Strony, oznaczonych jako poufne lub w przypadku których okoliczności przekazania informacji wskazują na obowiązek zachowania takich informacji w poufności (informacje poufne) zgodnie z postanowieniami niniejszego ustępu:
    a) Informację poufną stanowią informacje uzyskane przez Stronę od drugiej Strony w związku z wykonywaniem czynności określonych w Umowie, których ujawnienie osobom trzecim może narazić Stronę przekazującą te informacje na szkodę, w szczególności informacje

stanowiące tajemnicę handlową i tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji oraz wszystkie informacje uzyskane w związku z realizacją zadań określonych Umową, w szczególności:

- treść i zawartość Zgłoszeń Serwisowych,
- treść komunikatów publikowanych w aplikacji do zgłoszeń serwisowych,
- dane osobowe,
- dane dotyczące zabezpieczeń,
- dane finansowe Zamawiającego oraz jego kontrahentów.

b) Strony zobowiązane są zapobiec ujawnianiu, czy rozpowszechnianiu informacji poufnych drugiej Strony, uzyskanych w toku realizacji Umowy. Każda ze Stron zobowiąże wszystkie osoby związane z wykonywaniem Umowy do zachowania poufności informacji poufnych drugiej Strony.

c) Obowiązek zachowania informacji poufnych obowiązuje Strony przez okres wskazany w samych informacjach, towarzyszących im dokumentach lub mediach z wykorzystaniem których zostały przekazane lub jeżeli okres nie został wskazany, przez okres trzech lat po rozwiązaniu lub wygaśnięciu Umowy, bez względu na sposób i tryb rozwiązania lub wygaśnięcia. Zwolnienia Strony z obowiązku zachowania poufności dokonuje ta Strona, której dotyczą informacje poufne, na piśmie pod rygorem nieważności.

d) Obowiązku zachowania poufności nie stosuje się do informacji:

- powszechnie znanych w momencie ich ujawnienia;
- otrzymanych przez Stronę, zgodnie z powszechnie obowiązującymi przepisami prawa, od podmiotu uprawnionego bez obowiązku zachowania poufności;
- które w momencie ich przekazania były już znane Stronie bez obowiązku zachowania poufności;
- w stosunku do których Strona uzyskała pisemną zgodę drugiej Strony na ich ujawnienie (pod rygorem nieważności zgody na ujawnienie uzyskanej w innej niż pisemna formie).

e) Jeżeli ujawnienie informacji poufnej nastąpić ma na żądanie sądu lub innego upoważnionego organu władzy państwowej działającego zgodnie z prawem, Strona obowiązana do ujawnienia informacji poufnych zawiadomi o tym bezzwłocznie drugą Stronę, umożliwiając jej zajęcie stanowiska co do konieczności, zakresu lub formy takiego ujawnienia.

f) Jeżeli Strony nie postanowią inaczej na piśmie, wszelkie informacje poufne pozostaną własnością Strony, która ujawnia informacje poufne i zostaną jej zwrócone lub na jej pisemne żądanie zniszczone w dniu wygaśnięcia lub rozwiązania Umowy lub w innym terminie uzgodnionym przez upoważnionych przedstawicieli Stron.

§ 8

Gwarancja

1. Wykonawca udziela gwarancji na oferowany sprzęt wynoszący 60 miesięcy, z możliwością jej przedłużenia o 24 miesiące. Termin gwarancji będzie liczony od dnia podpisania protokołu końcowego.

2. Zamawiający dopuszcza, że usługi gwarancyjne sprzętu mogą być realizowane przez inny podmiot niż Wykonawca, posiadający autoryzację producenta oraz ISO 9001:2008 na świadczenie usług serwisowych.
3. Wykonawca zobowiązuje się do zapewnienia Zamawiającemu możliwości sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobierania uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
4. Wykonawca zobowiązuje się do zapewnienia aktualizacji i wparcia technicznego w zakresie zakupionego oprogramowania w okresie 60 miesięcy od dnia podpisania bezusterkowego Protokołu odbioru końcowego przedmiotu zamówienia.
5. Usługi gwarancyjne w zakresie oprogramowania świadczone będą w dni robocze w godzinach 8-16, z wyłączeniem dni ustawowo wolnych od pracy z czasem reakcji:
   - przy błędzie krytycznym do 8h od momentu zgłoszenia;
   - przy błędach zwykłych do 12h roboczych od momentu zgłoszenia.

6. Zgłoszenia o których mowa powyżej będą dokonywane za pomocą aplikacji serwisowej udostępnionej pod adresem……. lub elektronicznie poprzez wysłanie zgłoszenia na adres ……., a poza godzinami i dniami roboczymi, telefonicznie pod numerem tel.: ……,
   w systemie 24x7x365.

§ 9

Zmiany Umowy

1. Wszelkie zmiany niniejszej Umowy, z zastrzeżeniem § 3 dotyczącego zmiany osób upoważnionych do kontaktu ze strony Zamawiającego i Wykonawcy, muszą być dokonane stosownym aneksem do Umowy sporządzonym w formie pisemnej, pod rygorem nieważności.
2. Z uwzględnieniem art.455 ust.1 pkt 1 Ustawy zmiany Umowy są dopuszczalne w następujących okolicznościach:
   a) zmian wynikających z przekształceń własnościowych w przypadku połączenia, przejęcia, wydzielenia, przekształcenia w inną formę organizacyjno-prawną,
   b) zmian organizacyjno-technicznych, zmiany adresu, zmiany banku obsługującego Wykonawcę lub Zamawiającego,
   c) zastąpienia przedmiotu Umowy w części lub w całości produktem o lepszych parametrach w porównaniu do parametrów określonych w ofercie, przy czym cena tego produktu nie może być wyższa niż cena oferowanego przedmiotu zamówienia,
   d) zastąpienia sprzętu/oprogramowania, który ma być dostarczony w ramach realizacji niniejszej Umowy, sprzętem/oprogramowaniem nowym posiadającym co najmniej takie same parametry, jakie posiadał sprzęt/oprogramowanie będący podstawą wyboru oferty Wykonawcy w przypadku zakończenia produkcji lub wstrzymania produkcji sprzętu/oprogramowania, lub dystrybucji wyrobu będącego przedmiotem zamówienia, który ma być dostarczony, pod warunkiem, że Zamawiający zaakceptuje zmianę sprzętu/oprogramowania, a cena wprowadzonego sprzętu nie ulegnie zwiększeniu,

e) zmiany numerów katalogowych produktu, jeżeli Wykonawca zaoferuje przedmiot Umowy o tożsamych lub lepszych parametrach, nastąpi zmiana numerów katalogowych przez producenta przedmiotu Umowy,

f) zmiany terminu realizacji zamówienia w sytuacji, gdy zmiana ta wynika z przyczyn niezależnych od Wykonawcy, polegających w szczególności na: nieprzygotowaniu miejsca dostawy przez Zamawiającego w odpowiednim czasie, zmianie terminu dokonanej przez Zamawiającego

z uwagi na nie dające się przewidzieć okoliczności w tym potwierdzonego przez dystrybutorów/producentów przerwania w łańcuchu dostaw, niemożliwości przeprowadzenia szkolenia pracowników Zamawiającego z przyczyn leżących po stronie Zamawiającego

w szczególności nieobecności spowodowanej chorobą osób szkolonych, w przypadku wystąpienia opisanej w ustępach poniżej Siły Wyższej.

g) ustawowej zmiany stawki podatku VAT, z przyczyn wynikających ze zmiany przepisów lub wprowadzonych drogą decyzji właściwych organów administracji państwowej,

h) sytuacji, których Zamawiający nie jest w stanie przewidzieć w chwili podpisania Umowy, a zmiana ta jest korzystna dla Zamawiającego lub leży w interesie publicznym,

i) zastąpienia dotychczasowego Wykonawcy nowym Wykonawcą - w wyniku sukcesji, wstępując w prawa i obowiązki Wykonawcy, w następstwie przejęcia, połączenia, podziału, przekształcenia, upadłości, restrukturyzacji, dziedziczenia lub nabycia dotychczasowego Wykonawcy lub jego przedsiębiorstwa, o ile nowy Wykonawca spełnia warunki udziału w postępowaniu, nie zachodzą wobec niego podstawy wykluczenia oraz nie pociąga to za sobą innych istotnych zmian Umowy, a także nie ma na celu uniknięcia stosowania przepisów ustawy.

3. Strony Umowy nie będą odpowiedzialne za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy spowodowane przez okoliczności traktowane jako Siła Wyższa.
4. Dla celów Umowy ''Siła Wyższa" oznacza zdarzenie zewnętrzne, pozostające poza kontrolą Stron oraz niewiążące się z zawinionym działaniem Stron, którego Strony nie mogły przewidzieć i które uniemożliwia proces realizacji Umowy. Takie zdarzenia obejmują w szczególności: wojnę, rewolucję, pożary, powodzie, zagrożenia epidemiczne, trzęsienie ziemi.
5. W przypadku zaistnienia Siły Wyższej, Strona, której taka okoliczność uniemożliwia lub utrudnia prawidłowe wywiązanie się z jej zobowiązań, niezwłocznie powiadomi drugą Stronę o takich okolicznościach i ich przyczynie (odpowiednio udokumentuje zaistniałe okoliczności). Wówczas Strony niezwłocznie ustalą zakres, alternatywne rozwiązanie i sposób realizacji Umowy. Strona zgłaszająca okoliczności musi kontynuować realizację swoich zobowiązań wynikających z Umowy w takim stopniu, w jakim jest to możliwe i musi szukać racjonalnych środków alternatywnych dla realizowania zakresu, jaki nie podlega wpływowi Siły Wyższej.
6. Jeżeli Siła Wyższa, będzie trwała nieprzerwanie przez okres 180 dni lub dłużej, Strony mogą w drodze wzajemnego uzgodnienia rozwiązać Umowę bez nakładania na żadną ze Stron dalszych zobowiązań oprócz płatności należnych z tytułu prawidłowo wykonanych usług.
7. Stan Siły Wyższej powoduje odpowiednie przesunięcie terminów realizacji Umowy chyba, że

Strony postanowiły inaczej.

§ 10

Odstąpienie od Umowy

1. Odstąpienie od Umowy przez Zamawiającego może nastąpić w przypadku:
   a) dostarczenia przez Wykonawcę przedmiotu Umowy niezgodnego z ofertą,
   b) dostarczenia przedmiotu Umowy ze zwłoką przekraczającą 30 dni, niezależnie od możliwości naliczenia kar umownych.
2. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
3. W przypadku odstąpienia od Umowy, o którym mowa w ust. 2, Wykonawca może żądać jedynie wynagrodzenia za część Umowy wykonanej do dnia odstąpienia od Umowy.
4. Odstąpienie od Umowy w trybie § 10 ust. 1 winno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia złożonego w terminie 30 dni od powzięcia informacji o zaistnieniu przesłanek do odstąpienia.

§ 11

Kary umowne

1. W razie niewykonania lub nienależytego wykonania Umowy Wykonawca jest obowiązany zapłacić Zamawiającemu karę umowną w następujących przypadkach:
   a) w wysokości 20% łącznego wynagrodzenia brutto określonego w § 6 ust. 1, w przypadku odstąpienia przez Wykonawcę lub Zamawiającego od części lub całości Umowy lub innego sposobu rozwiązania Umowy z powodu okoliczności, za które Wykonawca ponosi wyłączną odpowiedzialność, w tym wskazanych w § 10 ust.1 pkt a), b);
   b) w wysokości 1 % łącznego wynagrodzenia brutto określonego w § 6 ust. 1, za każdy dzień zwłoki w przypadku nieterminowej realizacji zamówienia zgodnie z terminem określonym w § 5 ust. 1 niniejszej Umowy
   c) w wysokości 1 % łącznego wynagrodzenia brutto określonego w § 6 ust. 1, za każdy dzień zwłoki w przypadku nieterminowej realizacji usług gwarancyjnych, o których mowa w § 8 niniejszej Umowy.
2. Zamawiający może dochodzić odszkodowania przewyższającego wysokość kar umownych, z zastrzeżeniem ust. 3.
3. Całkowita wzajemna odpowiedzialność odszkodowawcza Wykonawcy, bez względu na podstawę prawną roszczenia (tj. zarówno z tytułu niewykonania lub nienależytego wykonania Umowy, jak i z tytułu czynu niedozwolonego), ograniczona jest do wartości Umowy i nie obejmuje utraconych korzyści Zamawiającego.
4. Łączna wysokość kar umownych naliczonych na podstawie § 11 ust. 1 nie może przekroczyć 30 % łącznej wartości Umowy brutto określonej w § 6 ust. 1 Umowy.

§ 12

Podwykonawcy

Wykonawca oświadcza, że przedmiot zamówienia wykona własnymi siłami z/ bez udziału podwykonawców/z udziałem podwykonawców*tj. ……

§ 13

Postanowienia końcowe

1. Umowa wchodzi w życie z dniem zawarcia.
2. Spory powstałe na tle realizacji niniejszej Umowy strony poddają pod rozstrzygnięcie sądu właściwego dla siedziby Zamawiającego.
3. W sprawach nieuregulowanych w niniejszej umowie będą miały zastosowanie właściwe przepisy Kodeksu Cywilnego oraz ustawy z dnia 19 września 2019 r. Prawo Zamówień Publicznych, SWZ oraz oferta Wykonawcy.
4. Załączniki do Umowy stanowią integralną część Umowy.
5. Umowę niniejszą sporządzono w dwóch jednobrzmiących egzemplarzach, oba na prawach oryginału, po jednym dla każdej ze Stron.

WYKONAWCA ***ZAMAWIAJĄCY***

Załączniki:

1. Załącznik nr 1 – Szczegółowy opis przedmiotu zamówienia
2. Załącznik nr 2 – Formularz oferty