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:

10/08/2022

Włoszczowa, dnia 31.08.2022 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-maill: **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 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r.)***, w tym:
   a) Dostawa serwera kopii zapasowych wraz z instalacją i konfiguracją,
   b) Dostawa oprogramowania klasy Security Information Event Management i Security Orchestration, Automation And Response,
   c) Dostawa oprogramowania do backupu,
   d) Dostawa licencji Microsoft Office - 40 sztuk
   e) Wykonanie usług wdrożeniowych w zakresie dostarczanego oprogramowania

f) 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 68/2022/BBIICD na podstawie umowy Nr 5/ZBIiCD.3120.5.2022 z dnia 03.08.2022 r. zawartej z Narodowym Funduszem Zdrowia.

VI. Opis części zamówienia:

1. Zamawiający nie podzielił zamówienia na części i nie dopuszcza składania ofert częściowych. Przedmiot zamówienia dotyczy dostawy oprogramowania i sprzętu podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych wraz z wykonaniem usług podnoszących bezpieczeństwo systemów IT stanowiące jedną funkcjonalno-użytkową całość. Poszczególne moduły oprogramowania muszą być ze sobą kompatybilne. Nie jest możliwe dopuszczenie ofert częściowych na poszczególne dostawy i instalacje, bo dokonany tak podział mógłby skutkować brakiem możliwości zapewnienia prawidłowego funkcjonowania całego systemu komputerowego i brakiem możliwości wyegzekwowania od wykonawców poszczególnych części uwzględnienia reklamacji w tym zakresie. Nadto z uwagi na fakt, iż pozyskane na ten cel środki z NFZ należy wydatkować do końca roku, konieczne jest bardzo sprawne i szybkie zakończenie zadania, co w sytuacji realizacji go przez kilku wykonawców może okazać się niewykonalne.

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 90 dni (ok. 3 miesiące) od dnia zawarcia umowy - **jest to termin maksymalny realizacji zamówienia**.

W przypadku, gdy w kryterium czas wdrożenia systemu SIEM Wykonawca zaproponuje krótszy termin, to w ramach umowy będzie zobowiązany do realizacji wdrożenia systemu 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:

w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, dostarczył licencję i wdrożył system klasy SIEM o wartości minimum 250 000,00 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</u>**

<u>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, dostarczył licencję i wdrożył system klasy SIEM o wartości minimum 250 000,00 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 polegającego na dostawie licencji i wdrożeniu systemu klasy SIEM.

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 Szwarc / Agnieszka Bukowska – Dział Obsługi Administracyjno-Technicznej - w sprawach proceduralnych tel. 41 3883837 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 09.09.2022r. godziny 10:00.
2. Termin związania ofertą upływa w dniu 07.10.2022 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. 09.09.2022 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).

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

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.

Kryterium czas wdrożenia systemu SIEM – 40%

Zamawiający wymaga, aby czas wdrożenia systemu SIEM był nie dłuższy niż 90 dni od daty zawarcia umowy. Wykonawca w formularzu ofertowym może określić krótszy czas wdrożenia systemu SIEM, za który może uzyskać dodatkowe punkty w przedmiotowym kryterium.

Minimalny czas wdrożenia systemu SIEM, za który można otrzymać maksymalna liczbę punktów wynosi 40 dni.

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

Czas wdrożenia systemu w terminie do 40 dni od daty zawarcia umowy	40 punktów
Czas wdrożenia systemu powyżej 40 do 70 dni od daty zawarcia umowy	20 punktów
Czas wdrożenia systemu powyżej 70 do 90 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 wdrożenia systemu).
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**;
2. 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"**, prowadzonym w trybie podstawowym bez negocjacji na podstawie art. 275 pkt 1;
3. 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);

4. 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;
5. 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;
6. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
7. 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

1. Serwer

Serwer - 1 szt.		
Wymagane minimalne parametry techniczne		**Tak, podać**
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.	
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
Procesor	Zainstalowany jeden procesor 8-rdzeniowy, min. 3.2 GHz (Turbo Speed min. 3.6 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 19984 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.	
RAM	128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling	
Gniazda PCI	- minimum dwa sloty PCIe w tym minimum jeden x16 generacji 4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Zainstalowana dodatkowa karta posiadająca 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ .	
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 2 dyski SAS o pojemności min. 900GB, 12Gb, Hot-Plug 15K Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min.	

	480GB Hot-Plug z możliwością konfiguracji RAID 1. Zainstalowany dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.	
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.	
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,	
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200	
Zasilacze	Redundantne, Hot-Plug min. 800W każdy	
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem	
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację	

	użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022	
Warunki gwarancji	5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego - dokumenty należy dostarczyć na wezwanie. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty należy dostarczyć na wezwanie. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień	

	mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	

2. Oprogramowanie biurowe

Oprogramowanie biurowe - 40 szt.	
Wymagane minimalne funkcjonalności	**Tak, podać**
Oprogramowanie Microsoft Office 2021 Home & Business lub równoważne: 1) Licencja i oprogramowanie musi być nowe, nieużywane, nigdy wcześniej nieaktywowane. 2) Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. 3) Zamawiający nie dopuszcza dostawy licencji typu OEM. 4) Licencje na oprogramowanie biurowe muszą pozwalać na przenoszenie oprogramowania pomiędzy stacjami roboczymi (np. w przypadku wymiany stacji roboczej). 5) Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta. Interfejs użytkownika w pełnej polskiej wersji językowej. 6) Możliwość automatycznej instalacji komponentów pakietu (przy użyciu instalatora systemowego). 7) Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem: system operacyjny Microsoft Windows 10, Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 2016, Microsoft Office 2019, Microsoft Windows Server 2008, Microsoft Windows Server 2012, Microsoft Windows Server 2016, Microsoft Windows Server 2019 8) Możliwość zintegrowania uwierzytelnienia użytkowników z usługą katalogową (Active Directory). 9) Tworzenie i edycja dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: - posiada kompletny i publicznie dostępny opis formatu, - posiada zdefiniowany układ informacji w postaci XML, - umożliwia wykorzystanie schematów XML, - wspiera w swojej specyfikacji podpis elektroniczny w formacie XADES, - możliwość automatycznego odzyskiwania dokumentów elektronicznych w wypadku	

nieoczekiwanego zamknięcia aplikacji, np. w wyniku wyłączenia zasilania komputera, - prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: DOC, DOCX, XLS, XLSX, XLSM, PPT, PPTX, MDB, ACCDB, w tym obsługa formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013 i MS Office 2016, bez utraty danych oraz bez konieczności formatowania dokumentów, - wszystkie aplikacje w pakiecie oprogramowania biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzania i wymiana danych, posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi), - edytor tekstowy powinien zapewnić możliwość tworzenia dokumentów dostępnych cyfrowo. Powinien zawierać narzędzie „inspektor dostępności" sprawdzające część wymagań dostępności w wytworzonym dokumencie. Edytor powinien pozwalać również na opisywanie osadzonych wszelakich obiektów w tekście (np.: tabela, wykres, grafika itp.) tekstem alternatywnym. - Pakiet zintegrowanych aplikacji biurowych musi składać się co najmniej z następujących aplikacji: − edytora tekstów, − arkusza kalkulacyjnego, − narzędzia do przygotowywania i prowadzenia prezentacji, − narzędzia do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). 10) W przypadku zaoferowania oprogramowania równoważnego powinno ono spełnić wszystkie wymagania opisane w pkt. od 1) do 9). 11) Zamawiający zastrzega sobie prawo weryfikacji, na etapie dostawy, czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem. W powyższym celu zamawiający może zwrócić się do przedstawicieli producenta danego oprogramowania z prośbą o weryfikację czy oferowane oprogramowanie i materiały do niego dołączone są oryginalne. W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych. Ponadto, powyższe informacje zostaną przekazane producentowi oraz odpowiednim służbom i organom ścigania. 12) Przedstawione powyżej zastrzeżone znaki handlowe służą jedynie do celów identyfikacyjnych i do określenia kompatybilności.	

3. Serwerowy System Operacyjny

Serwerowy System Operacyjny - 1 szt.	
Wymagane minimalne funkcjonalności	**Tak, podać**
Licencja musi uprawniać do uruchamiania SSO na dostarczanym serwerze w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów	

wirtualizacji. Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy. 1) Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym 2) Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych. 4) Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Graficzny interfejs użytkownika. 16) Zlokalizowane w języku polskim, następujące elementy:	

• menu, • przeglądarka internetowa, • pomoc, • komunikaty systemowe. 17) Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 18) Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 19) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 20) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 21) Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: • Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: • Dystrybucję certyfikatów poprzez http • Konsolidację CA dla wielu lasów domeny, • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). • Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.	

• Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersji 6 (IPv6), • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • Obsługi ramek typu jumbo frames dla maszyn wirtualnych, • Obsługi 4-KB sektorów dysków, • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) • Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 22) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 23) Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 24) Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 25) Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.	

4. Oprogramowanie Wirtualizacyjne

Oprogramowanie Wirtualizacyjne - 1 kpl.	
Wymagane minimalne funkcjonalności	**Tak, podać**
Licencje oprogramowania VMware vSphere 7 Essentials Kit, 3 lat wsparcia licencja wieczysta – lub oprogramowanie równoważne. Opis równoważności: Konsolidacja 1. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana	

bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego. 2. Rozwiązanie musi zapewnić wymóg obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest wymóg przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna. 2. Oprogramowanie do wirtualizacji musi zapewnić wymóg skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej. 3. Oprogramowanie do wirtualizacji musi zapewnić wymóg przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych. 4. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 5. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 6. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, MS Windows 7/8/10) , Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, SLES 11, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, Mac OS X. 7. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. 8. Dostęp do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska. 9. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root. 10. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania. 11. Rozwiązanie musi zapewnić wymóg monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych. 12. Rozwiązanie musi zapewniać wymóg konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi. 13. Oprogramowanie do wirtualizacji musi zapewnić wymóg klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 14. Oprogramowanie zarządzające musi posiadać wymóg przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Active Directory, Open LDAP.	

5. Motor bazy danych

Motor bazy danych - 10 szt.	
Wymagane minimalne funkcjonalności	**Tak, podać**
1. Baza danych musi umożliwiać pracę na dedykowanej platformie wirtualizacyjnej z przydzieloną odpowiednią ilością licencji dla CPU. 2. Możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych. 3. Oprogramowanie musi być dostępne na platformy sprzętowe i systemowe - 64-bitowe platformy Unix, Linux 64-bit, MS Windows 64-bit. 4. Oprogramowanie nie może mieć limitów na ilość przechowywanych danych – zarówno tekstowych, jak i multimedialnych. 5. Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji powinien pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, z kolei spójny odczyt nie powinien blokować możliwości wykonywania zmian. Oznacza to, że modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. 6. Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana. 7. Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). 8. Możliwość migracji zestawu znaków bazy danych do Unicode 9. Możliwość redefiniowania przez Zamawiającego ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych. 10. Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych 11. Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych 12. Wsparcie protokołu XA 13. Wsparcie standardu JDBC 3.0	

14. Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.

15. Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.

16. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).

17. Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu

18. Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych, jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).

19. Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej)

20. Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).

21. W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek

22. Możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu wewnętrznego w stosunku do bazy danych.

23. Baza danych powinna umożliwiać wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowania konta przez administratora bądź w przypadku

przekroczenia limitu nieudanych logowań. 24. Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. 25. Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServeitd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online 26. Zamawiający dopuszcza zastosowanie licencji typu Application Specific Full Use licencjonowanej na użytkownika.	

6. Oprogramowanie SIEM

Motor bazy danych - 10 szt.	
Wymagane minimalne funkcjonalności	**Tak, podać**
1. System musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji. 2. System musi zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą. 3. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.	

4. Dostarczone rozwiązanie musi być systemem klasy SOAR (Security Orchestration, Automation And Response). Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania. 5. Interfejs systemu elektronicznej dokumentacji musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami. 6. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej. 7. System musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians). 8. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum: na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego i tabelarycznego. 9. Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji. 10. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci. 11. System musi pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, MS Word, MS Excel, jpg, png. 12. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja. 13. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego. 14. Dla zarejestrowanych zdarzeń/ incydentów system automatycznie wyznaczy ścieżkę ataku i	

zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.

15. Dla zdarzeń zawierających adresy IP interfejs musi umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, powiązane incydenty, lokalizacja.

16. Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).

17. Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.

18. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

19. W ramach obsługi zdarzeń/incydentów/podatności system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na organizację w przypadku materializacji zagrożenia.

20. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np.: przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.

21. System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.

22. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.

23. System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.

24. System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci musi pozwalać m.in. na:

    - wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem

analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny, • wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia, • wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia, • wyświetlanie lokalizacji zasobów określonego rodzaju, • wyświetlanie najbardziej narażonych zasobów teleinformatycznych, • wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie. 25. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych). 26. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE. 27. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym. 28. System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych. 29. System musi umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System musi umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np: login, adres IP, aplikacja. 30. System musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych, system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji. 31. System musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w scenariuszach obsługi incydentów. Scenariusze obsługi incydentów muszą być uzależnione od ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych). 32. System musi umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (ang. Playbook). 33. System musi zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń,	

analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi:

- wzbogacanie danych kontekstowych,
- gromadzenie artefaktów danych związanych z incydentem,
- współpraca z innymi członkami zespołu,
- komunikacja w ramach zespołu,
- wykonywanie czynności związanych z reakcją na incydent,
- raportowanie przebiegu incydentu.

34. System musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów/podatności. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.

35. System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook).

36. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.

37. System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego.

38. System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IoC.

39. System musi umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów.

40. System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu.

41. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm musi umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.

42. Parsowanie warunkowe i hierarchiczne musi być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich w warunkach.

43. Proces normalizacji musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.

44. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania. 45. System musi zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email. 46. Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach. 47. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. 48. Normalizacja musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware, vulnerability. 49. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. 50. System musi posiadać predefiniowany zestaw parserów. 51. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych oraz formaty JSON, XML, CIS, LEEF, Syslog. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia. 52. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. 53. System musi umożliwiać definiowanie zakresu i czasu uczenia, np.: analiza logowania użytkowników po godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu. 54. System musi mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence, Active Directory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika. 55. System musi posiadać funkcję „automatycznej korelacji”, tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego”, będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły. 56. System musi zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.	

57. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych. 58. Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego). 59. Rozwiązania SIEM/UEBA, SOAR, narzędzia elektronicznej dokumentacji, narzędzie analizy ryzyka cyberzagrożeń oraz baza wiedzy mogą być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. Dostarczone rozwiązanie/ rozwiązania nie mogą działać w oparciu o technologię typu open-source. 60. Interfejs użytkownika Systemu musi być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych. 61. Funkcjonowanie rozwiązania musi być oparta w całości o architekturę „on-premise”, w której przetwarzane dane nie są przesyłane poza infrastrukturę Zamawiającego. 62. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x). 63. Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa. 64. System musi zapewniać możliwość współpracy z popularnymi bazami danych, a w tym co najmniej z: MS SQL lub Oracle. 65. System powinien umożliwiać nadawanie uprawnień do obiektów/modułów systemu dla poszczególnych operatorów lub grup operatorów. 66. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. 67. System musi dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD, minimum to: nazwa użytkownika, login, e-mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane. 68. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać	

możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

69. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).

70. System musi być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.

71. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.

72. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK.

73. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

74. Tworzenie raportów PDF musi posiadać opcje automatycznego harmonogramu, który w zadanym wcześniej momencie pozwoli na wysyłkę utworzonego raportu do zdefiniowanych odbiorców poczty email. Konfiguracja harmonogramu tworzenia raportów PDF i ich wysyłki powinna być dostępna poprzez graficzny interfejs użytkownika.

75. System musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.

76. System musi zapewniać klasyfikację zdarzeń za pomocą notacji punktowej definiującej ich poziom zagrożenia (ryzyko).

77. Interfejs systemu powinien umożliwiać z poziomu jednego okna widoku weryfikację wszystkich działań użytkownika na osi czasu, które spowodowały wzrost ryzyka. Z poziomu tego widoku system umożliwi przejście do opisu konkretnego zdarzenia.

78. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. usługi zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.

79. System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.

80. System musi automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych, konta serwisowe, użytkowników uprzywilejowanych, użytkowników w randze kierowniczej i zarejestrowane stacje robocze

celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu. 81. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach. 82. System musi umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje. 83. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów. 84. System musi umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany). 85. System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności. 86. System powinien mieć logikę automatycznego przypisywania zgłoszeń, minimum na podstawie dostępności operatora, jego obciążenia, oraz cech zasobu którego dotyczy incydent, minimum typ zasobu (np.: serwer lub stacja robocza), krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. 87. System musi umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników. 88. System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników. 89. System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamknięcie głównego incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach. 90. System musi pozwalać na określenie automatycznych oraz inicjowanych przez operatora reakcji na incydenty bezpieczeństwa i/lub zdarzenia, polegających na integracji z systemami zewnętrznymi w celu uzyskania dodatkowych informacji, dotyczących incydentu/zdarzenia lub podjęcia akcji zapobiegawczych. 91. System musi umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.). 92. System musi umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów	

93. System musi pozwalać na zbieranie danych i reputacji z systemów klasy Threat Intelligence minimum to IP, FQDN, URL, Hash. 94. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub/i PowerShell), na skonfigurowanie nowych, nie uwzględnionych przez producentów rozwiązania możliwości integracyjnych z zewnętrznymi systemami. 95. System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu i ilości incydentów, które są z nimi powiązane. 96. System musi mieć możliwość automatycznego informowania o zmianie statusu incydentu (minimum: wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu). 97. System powinien umożliwiać ustawienie parametrów SLA bazując na ustalonym automatycznie priorytecie zdarzania/incydentu/podatności. System musi dokonywać automatycznego pomiaru tych czasów i weryfikacji ich do zdefinowanych wymagań SLA. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu. 98. System powinien umożliwiać dodawanie, modyfikację i usuwanie umów SLA, które zawierają co najmniej następujące parametry: data rozpoczęcia i zakończenia obowiązywania umowy, jednostka organizacyjna (struktura jednostek), której dotyczy umowa, lista usług z katalogu usług, których dotyczy umowa. 99. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników. Silnik skanujący, będący źródłem podatności musi zostać dołączony do oferty systemu bezpieczeństwa. 100. Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem. 101. System musi automatycznie ustalać priorytety podatności w odniesieniu do ważności podatnych systemów IT dla organizacji oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera. 102. System powinien uwzględniać w ocenie zdarzeń i incydentów, informacje o podatnościach technicznych wykrytych przez narzędzia do zarządzania podatnościami zarówno przez import raportu jak i integrację przez API. 103. System musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów. 104. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (playbook). 105. System SIEM oraz wszystkie moduły towarzyszące muszą umożliwiać równoczesną pracę co	

najmniej 10 operatorów oraz objąć monitoringiem min. 200 zasobów IT. Przez zasób IT rozumie się serwery fizyczne lub serwery wirtualne oraz komputery użytkowników. Ilość danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz ilość kolektorów agregujących i parsujących nie może powodować zmian w zakresie licencjonowania. Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.

106. System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.

107. Zamówienie realizowane będzie w terminie do 90 dni (ok. 3 miesiące) od dnia zawarcia umowy - jest to termin maksymalny realizacji zamówienia.

108. Po zakończonym wdrożeniu należy zapewnić bezpłatne 3-dniowe certyfikowane szkolenia (5 x 8h) w zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać przeprowadzone dla maksymalnie 10 osób i uwzględniać informacje z zakresu wdrożonego systemu SIEM (m.in. zarządzanie incydentami bezpieczeństwa; kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.). Szkolenia muszą być zakończone egzaminem i certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.

109. Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. szczegółową dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).

Załącznik nr 1.
Szczegółowy zakres i wytyczne procesu wdrożenia systemu

1. Proces wdrożenia systemu powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania w max. okresie 3 miesięcy.

2. Proces wdrożeniowy podzielony zostanie są na 2 obszary:

   - Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);
   - Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
   - Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR;

3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:

- Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej);
- Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
  - konsultacje w przygotowaniu infrastruktury zamawiającego do instalacji systemu,
  - instalację lub import maszyny wirtualnej typu „software appliance”,
  - zestawienie połączenia zdalnego,
  - aktywację licencji,
  - wstępną konfigurację,
  - import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);
- Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
  - przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
  - uruchomienie reguł wykrywania;
- Prace audytowe, w tym:
  - pasywną analizę transmisji sieciowej:
  - ruch z/do serwerów webowych i aplikacyjnych,
  - ruch z/do serwerów baz danych,
  - ruch z/do serwerów pocztowych,
  - ruch z/do kontrolerów domenowych,
  - ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
  - ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,
  - konsultacje w ramach otrzymanych wyników;
  - zebranie danych audytowych wymaganych do sporządzenia raportu;
- Analizę podatności, w zakresie:
  - integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source;

- przygotowanie reguł priorytetów i importu krytycznych podatności;

- Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:
  - zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
  - potencjalne wektory ataków dla wykrytych zagrożeń;
  - wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
  - rekomendacja zabezpieczeń;
  - zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;
- Transfer wiedzy w formie spotkania podsumowującego, obejmujący interpretację przez analityka wyników analizy ujętej w raporcie z systemu;

4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:

- Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła zdarzeń obejmują:
  - zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);
  - sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam)
  - centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);
  - kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;
  - systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);
  - system SIEM
  - w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;

- Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;
- Podłączenie reguł detekcji;
- Podłączenie i konfiguracja mechanizmów UEBA:
  - integracja z Active Directory

- utworzenie profili użytkowników UBA - utworzenie profili hostów EBA - import reguł bezpieczeństwa UEBA, utworzenie customowych reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia - obserwacja i doprecyzowanie postępu uczenia maszynowego, wykluczenie/ dodanie nowych reguł zdarzeń użytkowników/ hostów. • Dostrojenie systemu, w tym reguł priorytetyzacji zdarzeń i incydentów, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji; 5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać kolejno: • Pracę z konsultantem (m.in wprowadzenie do scenariuszy wbudowanych w systemie, analizę wymaganych zmian związanych z dostosowaniem scenariuszy, pomoc przy generowaniu API KEY dla wbudowanych akcji) • Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi • Konfigurację mechanizmów powiadamiania	

7. Usługi

Wymagane minimalne parametry techniczne
1. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego. 2. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafach serwerowych rack, w sposób umożliwiający ich prawidłową wentylację. 3. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie wdrożenia. 4. W zakresie części serwerowej w ramach postępowania wymagane jest wykonanie następujących usług: • Instalacja, montaż i uruchomienie serwerów wirtualizacyjnych: 1. Montaż serwera w istniejącej szafie rackowej 2. Podłączenie serwera do sieci LAN i/lub SAN 3. Podłączenie serwera do zasilania 4. Inicjalne uruchomienie serwera • Implementacja zgodna z projektem:

5. Instalacja sprzętowa
6. Aktywacja zakupionego oprogramowania
7. Implementacja zaakceptowanej konfiguracji logicznej macierzy
8. Instalacja oprogramowania wirtualizacyjnego i archiwizacji danych
9. Instalacja serwerowego systemu operacyjnego oraz uruchomienie kontrolera domeny.
10. Konfiguracja oprogramowania wirtualizacyjnego i archiwizacji danych

5. Zamawiający wymaga wdrożenia mechanizmu pozwalającego na uruchomienie replikacji produkcyjnej bazy danych i utworzenie bazy typu standby. Baza ma być separowana od fizycznego środowiska. W łatwy sposób ma umożliwiać przejęcia funkcję bazy produkcyjnej. Mechanizm pozwalający na uruchomienie ciągłej replikacji produkcyjnej bazy danych na niezależnym od produkcyjnego środowisku infrastruktury. Rozwiązanie w pełni zabezpiecza działanie systemu. W przypadku awarii w łatwy sposób może przejąć funkcję bazy produkcyjnej. Odmiennie jak w przypadku kopii zapasowych wykonywanych w nocy, synchronizacja odbywa się w trybie ciągłym, dlatego replikowana baza zawiera dane tożsame z serwerem produkcyjnym.
6. Zamawiający dopuszcza zmianę konfiguracji maszyn wirtualnych, jeżeli nowe rozwiązanie zapewni podniesienie jakości działania systemu Eskulap i Impuls. Zamawiający wymaga, aby propozycje wykonawcy dotyczące konfiguracji infrastruktury zostały omówione i zaakceptowane przez zamawiającego przed wdrożeniem.

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:

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 wdrożenie systemu SIEM zrealizujemy w terminie …….. dni od podpisania Umowy.
6. Oświadczamy, że udzielamy gwarancji na oferowany sprzęt komputerowy na okres: …….. miesięcy.
7. Z naszej strony realizację zamówienia koordynować będzie: …… tel. ……, e-mail…….
8. Oferta zawiera/nie zawiera * informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji.
9. 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 ……
10. Oświadczam, że firma, którą reprezentuję jest: mikroprzedsiębiorstwem*****, małym przedsiębiorstwem *****, średnim przedsiębiorstwem***** dużym przedsiębiorstwem*.
11. Oświadczam, że zamierzam/nie zamierzam* powierzyć następującej części zamówienia …… podwykonawcom……..

12. 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

13. 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”** 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”,** 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”**, 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”**, 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.

…….

Załącznik nr 5 do SWZ

(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 klasy SIEM o wartości minimum 250 000,00 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”** 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”** 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

„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 …./…. /2022

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 ……2022 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 (Dz.U. z 2022,poz.1710)
Strony Umowy w wyniku tego rozstrzygnięcia ustalają, co następuje.

§ 1
Przedmiot Umowy

1. Przedmiotem Umowy 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 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r.)**, w tym:
    a. Dostawa serwera kopii zapasowych wraz z instalacją i konfiguracją,
    b. Dostawa oprogramowania klasy Security Information Event Management i Security Orchestration, Automation And Response,

c. Dostawa oprogramowania do backupu,
d. Dostawa licencji Microsoft Office - 40 sztuk,
e. Wykonanie usług wdrożeniowych w zakresie dostarczanego oprogramowania,
f. Wykonanie usług szkoleniowych dla pracowników Zamawiającego.

2. Szczegółowy opis dostaw i usług 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 dostarczy sprzęt, który jest fabrycznie nowy, nieużywany, wolny od wad fizycznych i prawnych i nie jest przedmiotem praw lub roszczeń osób trzecich.
4. Wraz ze sprzętem, 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. Wykonawca zobowiązuje się do wdrożenia przedmiotu umowy zgodnie z wytycznymi i zakresem określonym przez Zamawiającego w załączniku nr 1 do SWZ pn.,,Szczegółowy zakres i wytyczne procesu wdrożenia systemu".
5. Strony akceptują fakt, że usługi wdrożeniowe, szkoleniowe i serwisowe mogą być wykonywane poza siedzibą Zamawiającego lub zdalnie.
6. 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 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 na fakturze w terminie 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 Wykonawcą na rzecz Udzielającego Zamówienie 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 12 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. Określenie pojęć błędu krytycznego i zwykłego zawiera punkt 58 Część 6 Oprogramowanie SIEM Załącznika Nr 1 pn.,, Szczegółowy opis przedmiotu zamówienia".
6. Zgłoszenia o których mowa powyżej będą dokonywane na 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. Żadna ze Stron Umowy nie będzie odpowiedzialna 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 obowiązuje od dnia jej zawarcia (data określona w komparycji Umowy).
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