Znak postępowania: 16/ZP/2022

Sejny, 23.10.2022 r.

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa, z podziałem na 4 zadania dla SP ZOZ w Sejnach

w trybie
podstawowym zgodnym z przepisami wydanymi na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2022 r., poz. 1710 ze zm.) zwana dalej Pzp lub ustawą,

Biuletynie Zamówień Publicznych pod numerem **2022/BZP 00405218/01**
Strona internetowa prowadzonego postępowania www.szpital.sejny.pl **od 23.10.2022**

Termin składania ofert 31.10.2022 godz. 11.00
Termin otwarcia ofert 31.10.2022 godz. 11:30

Zakup finansowany ze środków Funduszu Przeciwdziałania COVID-19

Uwaga
Zamawiający nie ponosi kosztów przygotowania oferty przez Wykonawcę.

ZATWIERDZAM

.....

I. NAZWA I ADRES ZAMAWIAJĄCEGO

1. Nazwa i adres Zamawiającego:
   Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach
   ul. Dr. Edwarda Rittlera 2
   16-500 Sejny

Adres strony internetowej: www.szpital.sejny.pl
Faks do korespondencji: **(0-87) 51 72 335**
Tel. sekretariat: **(0-87) 51 72 314**
Tel. zamówienia publiczne: (0-87) 51 72 319
E-mail sekretariatu: **sekretariat@szpital.sejny.pl**
E-mail do korespondencji: zamowienia.publiczne@szpital.sejny.pl;
Korespondencja pisemna na adres:
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach
czynny w dni robocze od poniedziałku do piątku w godz. 7^{00} – 14^{35}.

2. **Osobami uprawnionymi do porozumiewania się z Wykonawcami jest Jolanta Szafranowska, tel. 87 5172 319 , Hubert Charkiewicz, tel. 660 473 075**
3. Postępowanie, którego dotyczy niniejsza Specyfikacja Warunków Zamówienia oznaczone jest znakiem **16/ZP/2022** - Wykonawcy we wszelkich kontaktach z Zamawiającym powinni powoływać się na ten znak.
4. Adres strony internetowej prowadzonego postępowania: https://miniportal.uzp.gov.pl

Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia: www.szpital.sejny.pl , https://miniportal.uzp.gov.pl

KOD CPV:

Zadanie 1

48710000-8 Pakiety oprogramowania do kopii zapasowych i odzyskiwania
48620000-0 Systemy operacyjne
72263000-6 Usługi wdrażania oprogramowania
72265000-0 Usługi konfiguracji oprogramowania

Zadanie 2
48761000-0 Pakiety oprogramowania antywirusowego
72263000-6 Usługi wdrażania oprogramowania
72265000-0 Usługi konfiguracji oprogramowania

Zadanie 3
32424000-1 Infrastruktura sieciowa
72263000-6 Usługi wdrażania oprogramowania
72265000-0 Usługi konfiguracji oprogramowania

Zadanie 4
30233160 - Jednostki pamięci taśmowej
30237360-0 Kasety z taśmą LTO

II. TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie o udzielenie zamówienia prowadzone jest na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U. z 2022 r. poz. 1710 ze zm.) „zwanej dalej ”ustawą Pzp”. Wartość szacunkowa zamówienia jest niższa od progów unijnych określonych na podstawie art. 3 ustawy Pzp.

2. Postępowanie o udzielenie zamówienia prowadzone jest w trybie podstawowym bez negocjacji, o którym mowa w art. 275 pkt 1 ustawy Pzp.

III. INFORMACJE OGÓLNE

1. Komunikacja w postępowaniu o udzielenie zamówienia i w konkursie, w tym składanie ofert, wniosków o dopuszczenie do udziału w postępowaniu lub konkursie, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między zamawiającym a wykonawcą, z uwzględnieniem wyjątków określonych w ustawie Pzp, odbywa się przy użyciu środków komunikacji elektronicznej. Przez środki komunikacji elektronicznej rozumie się środki komunikacji elektronicznej zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).
2. Ofertę, oświadczenia, o których mowa w art. 125 ust. 1 Pzp,, podmiotowe środki dowodowe, pełnomocnictwa, zobowiązanie podmiotu udostępniającego zasoby sporządza się w postaci elektronicznej, w ogólnie dostępnych formatach danych, w szczególności w formatach .txt, .rtf, .pdf, .doc, .docx, .odt. Ofertę, a także oświadczenia składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia składa się z 4 niepodzielnych zadań:

Nr zadania	Nazwa zadania
1.	Zakup i wdrożenie kompleksowej platformy systemu kopii bezpieczeństwa
2.	Zakup i wdrożenie systemu antywirusowego dla stacji roboczych i serwerów – centralnie zarządzanych, system klasy Endpoint Detection and Response (EDR) – 175 szt./3 lata
3.	Zakup i wdrożenie urządzenia typu Firewall – 1 szt./5 lat
4.	Zakup i wdrożenie biblioteki taśmowej – 1 szt.

2.Wykonawca może powierzyć wykonanie części zamówienia Podwykonawcom.

a) Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, podał nazwy, dane kontaktowe oraz przedstawicieli, podwykonawców zaangażowanych w realizację zamówienia, jeżeli są już znani.
b) Wykonawca jest obowiązany zawiadomić Zamawiającego o wszelkich zmianach w odniesieniu do informacji, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazać wymagane informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację zamówienia.

3.Szczegółowy opis przedmiotu zamówienia został zawarty w formularzu wymaganych parametrów.

4.Zamawiający informuje, iż ilekroć w SWZ i jej załącznikach przedmiot zamówienia jest opisany:

a) ze wskazaniem znaków towarowych, nazw własnych, patentów lub pochodzenia źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę to przyjmuje się, że wskazaniom takim towarzyszą wyrazy „lub równoważny". Oznacza to, że dopuszcza się zaoferowanie wyrobów nie gorszych niż opisywanych, tj. spełniających wymagania techniczne, funkcjonalne i jakościowe, co najmniej takie jak wskazane w dokumentacji niniejszego postępowania,
b) poprzez odniesienie się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy, to przyjmuje się, że dopuszcza się rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy „lub równoważne".

V. TERMIN WYKONANIA ZAMÓWIENIA

Zamawiający wymaga aby zamówienie było wykonane **do 01.12.2022 r.**

VI. INFORMACJE DODATKOWE

1. Informacje dotyczące oferty wariantowej, o której mowa w art. 92 ustawy Pzp:
   Zamawiający nie dopuszcza składania ofert wariantowych.
2. Informacja o przewidywanych zamówieniach, o których mowa w art. 214 ust. 1 pkt 8 ustawy Pzp.
   Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 8 ustawy Pzp.

3. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej, o której mowa w art. 308 ust. 1 ustawy Pzp.
4. Zamawiający dopuszcza składanie ofert równoważnych.
5. Zamawiający nie dopuszcza składania ofert częściowych.
6. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 pzp.
7. Zamawiający nie stawia wymagań w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2 ustawy Pzp.

VII. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu oraz spełniają warunki udziału w postępowaniu i wymagania określone w niniejszej SWZ.
   Zamawiający, na podstawie art. 112 ustawy Pzp określa następujące warunki udziału w postępowaniu:

a) zdolności do występowania w obrocie gospodarczym,
Opis spełnienia warunku:
Zamawiający nie określa wymagań w tym zakresie.

b) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów,
Opis spełnienia warunku:
Zamawiający nie określa wymagań w tym zakresie.

c) sytuacji ekonomicznej lub finansowej,
Opis spełnienia warunku:
Zamawiający nie określa wymagań w tym zakresie.

d) zdolności technicznej lub zawodowej
Opis spełnienia warunku:
Zamawiający nie określa wymagań w tym zakresie.

VIII.PODSTAWY WYKLUCZENIA WYKONAWCY Z POSTĘPOWANIA

1. Zamawiający wykluczy z postępowania o udzielenie zamówienia Wykonawcę, wobec którego zachodzą podstawy wykluczenia, o których mowa w:
   a) art. 108 ust 1 ustawy Pzp.
   b) art 109 ust 1 pkt 4 ustawy Pzp
   z zastrzeżeniem art. 110 ust. 2 ustawy Pzp.
2. Wykluczenie Wykonawcy nastąpi w przypadkach, o których mowa w art. 111 ustawy Pzp.
3. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania, ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.
4. Na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 r., poz. 835) z postępowania o udzielenie zamówienia publicznego na podstawie ustawy Pzp Zamawiający wyklucza:
   a) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   b) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
   c) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

Wykluczenie, o którym mowa w niniejszym punkcie następować będzie na okres ww. okoliczności. W przypadku wykonawcy lub uczestnika konkursu wykluczonego na podstawie art. 7 ust 1 ustawy (Dz. U. 2022 poz 835), Zamawiający odrzuca ofertę takiego Wykonawcy.

Zamawiający będzie weryfikował przesłankę wykluczenia, o której mowa w art. 7 ust 9 ustawy (Dz. U. 2022 poz 835) na podstawie:

a) Wykazów określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014,

b) Listy Ministra właściwego do spraw wewnętrznych obejmujących osoby i podmioty, wobec których są stosowane środki, o których mowa w art. 1 ustawy (Dz. U. 2022 poz 835)

IX. INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH

1. Wykonawca wraz z ofertą zobowiązany jest złożyć:
   a) **Załącznik nr 1 – Formularz ofertowy**
   b) **Załącznik nr 2 - Formularz wymaganych parametrów**
   c) **Załącznik nr 5 – Oświadczenia Wykonawcy**

d) **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.

e) **Pełnomocnictwo** - Jeśli ofertę lub inne oświadczenia składa osoba, która nie jest umocowana do reprezentacji wykonawcy (wykonawców wspólnie ubiegających się o udzielenie zamówienia, lub podmiotów udostępniających zasoby) do oferty należy załączyć pełnomocnictwo, określające zakres umocowania. Pełnomocnictwo musi być złożone w oryginale w postaci elektronicznej i opatrzone kwalifikowanym podpisem elektronicznym przez osoby uprawnione do reprezentowania odpowiednio wykonawcy, podmiotu, na którego zdolnościach lub sytuacji polega wykonawca, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego albo podwykonawcy. W przypadku gdy pełnomocnictwo zostało sporządzone jako dokument z podpisem odręcznym mocodawcy – przekazuje się kopię tego pełnomocnictwa w postaci elektronicznej potwierdzoną za zgodność z oryginałem kwalifikowanym podpisem elektronicznym przez mocodawcę lub notariusza. W przypadku gdy prawo do udzielenia pełnomocnictwa nie wynika z dokumentów dostępnych w ogólnodostępnych bezpłatnych bazach danych wskazanych przez wykonawcę - wraz z pełnomocnictwem należy złożyć, w oryginale w postaci dokumentu elektronicznego albo elektronicznej kopii dokumentu poświadczonej za zgodność z oryginałem, dokumenty, z których wynika uprawnienie osób udzielających pełnomocnictwa do reprezentowania danego podmiotu.

2. **Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę**, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych:
   W celu potwierdzenia braku podstaw wykluczenia Wykonawcy z udziału w postępowaniu:

a) **Oświadczenia wykonawcy w sprawie grupy kapitałowej**
   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 (Dz. U. z 2021 r.poz.275 ze zm), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenie 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.

b) **Informacji z Krajowego Rejestru Karnego** w zakresie art. 108 ust 1 pkt 1, 2 i 4 ustawy Pzp, wystawionej nie wcześniej niż 6 miesięcy przed jej złożeniem

c) **Odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej**, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;

3. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania, wezwać Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
4. Jeżeli zajdą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, Zamawiający może w każdym czasie wezwać Wykonawcę do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
5. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
6. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia Wykonawca składa, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
7. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

X. INFORMACJA DLA WYKONAWCÓW POLEGAJĄCYCH NA ZASOBACH PODMIOTÓW TRZECICH

1. Wykonawca, w celu potwierdzenia spełnienia warunków udziału w postępowaniu, może polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów trzecich, na zasadach określonych w art. 118–123 ustawy Pzp.
2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, zobowiązany jest:

a) złożyć 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. Zobowiązanie podmiotu udostępniającego zasoby lub inny podmiotowy środek dowodowy, musi potwierdzać, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określać 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 zadania, których wskazane zdolności dotyczą.

b) złożyć wraz z ofertą ”Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków”, podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby;

c) przedstawić na żądanie Zamawiającego podmiotowe środki dowodowe, określone SWZ, dotyczące tych podmiotów, na potwierdzenie, że nie zachodzą wobec nich podstawy wykluczenia z postępowania.

XI INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
2. Pełnomocnictwo należy dołączyć do oferty i powinno ono zawierać w szczególności wskazanie:
   a) postępowania o udzielenie zamówienie publicznego, którego dotyczy;
   b) wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia;
   c) ustanowionego pełnomocnika oraz zakresu jego umocowania.
3. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, dokument ”Oświadczenia o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału”, o którym mowa w Rozdziale IX SWZ, składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

XII. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ UDZIELANIA WYJAŚNIEŃ TREŚCI SWZ

1. W niniejszym postępowaniu komunikacja między Zamawiającym a Wykonawcami w tym składanie ofert, wniosków o dopuszczenie do udziału w postępowaniu lub konkursie, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między Zamawiającym a Wykonawcą, z uwzględnieniem wyjątków określonych w ustawie Pzp, odbywa się przy użyciu środków komunikacji elektronicznej. Przez środki komunikacji elektronicznej rozumie się środki komunikacji elektronicznej zdefiniowane w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344).
2. Do złożenia oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy ważnego kwalifikowanego podpisu elektronicznego, podpisu zaufanego lub podpisu osobistego.
3. Ilekroć w niniejszej SWZ jest mowa o:
   a) podpisie zaufanym – należy przez to rozumieć podpis, o którym mowa art. 3 pkt 14a ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j Dz.U. 2021 r., poz. 2070)
   b) podpisie osobistym – należy przez to rozumieć podpis, o którym mowa w art. z art. 2 ust. 1 pkt 9 ustawy z 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz.U. 2022 r., poz. 671).
4. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu 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 oraz rozporządzeniu 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.

5. Ofertę, wraz ze stanowiącymi jej integralną część załącznikami, składa się pod rygorem nieważności w formie elektronicznej lub postaci elektronicznej za pośrednictwem mini Portalu podpisaną kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
6. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
7. Zawiadomienia, oświadczenia, wnioski lub informacje Wykonawcy przekazują:
   - drogą elektroniczną: **zamowienia.publiczne@szpital.sejny.pl**;
   - poprzez Platformę **miniPortal, ePUAP** dostępne pod adresem: **https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal**
8. Rejestracja na Platformie, w tym złożenie oferty w formie elektronicznej, wymaga aby **Wykonawca, aby wziąć udział w elektronicznym postępowaniu o udzielenie zamówienia publicznego musi założyć konto na ePUAP.** Rejestracja i korzystanie z Platformy miniPortal zostały opisane w instrukcji użytkownika systemu, która dostępna jest pod adresem: **https://miniportal.uzp.gov.pl/Instrukcje**
9. Zgodnie z art. 67 ustawy Pzp Zamawiający podaje wymagania techniczne związane z korzystaniem z Platformy:
   - Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy: „Formularz złożenia, zmiany, wycofania oferty lub wniosku" i „Formularza do komunikacji" wynosi 150 MB.
   - Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z systemu miniPortal, znajdującego się od adresem: (https://miniportal.uzp.gov.pl/WarunkiUslugi) oraz Warunkach korzystania z elektronicznej platformy usług administracji publicznej (ePUAP), znajdujące się pod adresem: https://www.gov.pl/web/gov/warunki-korzystania.
10. W korespondencji kierowanej do Zamawiającego Wykonawcy powinni posługiwać się numerem przedmiotowego postępowania.
    Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
    Jeżeli wniosek o wyjaśnienie treści SWZ nie wpłynie w terminie, o którym mowa w punkcie powyżej, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ.
    Przedłużenie terminu składania ofert, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
    Treść zapytań wraz z wyjaśnieniami Zamawiający udostępni na stronie internetowej prowadzonego postępowania, bez ujawniania źródła zapytania.
    W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej prowadzonego postępowania.

XIII. WYMAGANIA DOTYCZĄCE WADIUM.

Zamawiający nie wymaga złożenia wadium.

XIV. TERMIN ZWIĄZANIA Z OFERTĄ.

1. Wykonawca pozostaje związany ofertą do dnia **29.11.2022 r.**
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, Zamawiający przed upływem tego terminu zwróci się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie terminu związania ofertą o wskazywany przez niego okres, nie dłuższy niż 30 dni.
4. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XV. OPIS SPOSOBU PRZYGOTOWANIA OFERT

Składanie ofert:

1. Wykonawca składa ofertę za pośrednictwem Formularza do złożenia lub wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób złożenia oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
2. **Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie do dnia 31.10.2022 r., do godz. 11:00.**
3. Wykonawca może złożyć tylko jedną ofertę.
4. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
5. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
6. Wykonawca po przesłaniu oferty za pomocą Formularza do złożenia lub wycofania oferty na „ekranie sukcesu" otrzyma numer oferty generowany przez ePUAP. Ten numer należy zapisać i zachować. Będzie on potrzebny w razie ewentualnego wycofania oferty.
7. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem Formularza do wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.
8. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

Otwarcie ofert.

1. **Otwarcie ofert nastąpi w dniu 31.10.2022 r. o godzinie 11:30.**
2. Otwarcie ofert jest niejawne.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informacją o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. 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.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
7. W toku dokonywania badania i oceny złożonych ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących ich treści.
8. Oferty, które nie zostaną odrzucone, zostaną poddane procedurze oceny zgodnie z kryterium oceny ofert określonym w niniejszej SWZ.
9. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie PZP oraz w SWZ, a ponadto uzyska największą liczbę punktów zgodnie z przyjętym kryterium oceny ofert.

XVI. OPIS SPOSOBU OBLICZANIA CENY.

1. W ofercie Wykonawca zobowiązany jest podać cenę za wykonanie całego przedmiotu zamówienia w złotych polskich (PLN), z dokładnością do 1 grosza, tj. do dwóch miejsc po przecinku.
2. W cenie należy uwzględnić wszystkie wymagania określone w niniejszej SWZ oraz wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia, a także wszystkie potencjalne ryzyka ekonomiczne, jakie mogą wystąpić przy realizacji przedmiotu zamówienia.
3. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich z dokładnością do dwóch miejsc po przecinku.
4. Wykonawca zobowiązany jest zastosować stawkę VAT zgodnie z obowiązującymi przepisami ustawy z 11 marca 2004 r. o podatku od towarów i usług.
5. Jeżeli złożona zostanie oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z 11 marca 2004 r. o podatku od towarów i usług, dla celów zastosowania kryterium ceny Zamawiający doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.
6. Wykonawca składając ofertę zobowiązany jest:
   a) poinformować Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
   b) wskazać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
   c) wskazać wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;

d) wskazać stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

XVII. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY.

1. Przy dokonywaniu wyboru najkorzystniejszej oferty Zamawiający stosować będzie niżej podane kryteria, które liczone będą zgodnie z poniższymi zasadami:

LP	NAZWA KRYTERIUM	WAGA
1	CENA	60 pkt
2	TERMIN WYKONANIA	40 pkt

Sposób obliczania wartości punktowej kryteriów:

1/ ***Kryterium nr 1 „Cena”*** oceniane będzie jak niżej

$$X = \frac{C_{min}}{C_o} \times 60 \text{ pkt.}$$

gdzie:
X – wartość punktowa ocenianego kryterium
Cmin – najniższa cena ze złożonych ofert
Co – cena ocenianej oferty

Maksymalna liczba punktów 60 pkt.

2/ ***Kryterium nr 2 „termin wykonania”*** oceniane będzie jak niżej:

do 01.12.2022 r. – 0 pkt
do 25.11.2022 r. – 20 pkt
do 20.11.2022 r. – 40 pkt

Uwaga: Maksymalna liczba punktów 40 pkt.

2. **Założenie:**

Zamawiający dla każdego zadania dokona oddzielnej oceny ofert.
1) Punktacja jaką otrzyma Wykonawca w ramach kryterium „**cena**” + kryterium „ **termin wykonania**” w niniejszym postępowaniu zostanie ustalona zgodnie ze wzorem określonym powyżej
2) 100 (waga kryterium „**cena**”+ kryterium „ **termin wykonania**”) – oznacza, że w postępowaniu można uzyskać max. 100 pkt. w ramach wyżej wymienionych dwóch kryteriów (100 pkt.)
3) Ocena końcowa danej oferty będzie sumą punktów uzyskanych przez ofertę w zakresie powyższych kryteriów liczonych dla każdego zadania oddzielnie. Za najkorzystniejszą zostanie uznana oferta z najwyższą liczbą punktów.

3. Zamawiający poprawi w ofercie:
a) oczywiste omyłki pisarskie,
b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
c) inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty
- niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
4. Jeżeli zaoferowana cena, lub jej istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia lub budzą wątpliwości Zamawiającego co do możliwości wykonania

przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, Zamawiający zażąda od Wykonawcy wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny, lub jej istotnych części składowych. Wyjaśnienia mogą dotyczyć zagadnień wskazanych w art. 224 ust. 3 ustawy Pzp.
5. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy.
6. Zamawiający odrzuci ofertę Wykonawcy, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdzi, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.
7. Zamawiający odrzuci ofertę Wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają rażąco niskiej ceny tej oferty.

XVIII. UDZIELENIE ZAMÓWIENIA

1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszej SWZ i została oceniona jako najkorzystniejsza | w oparciu o podane w niej kryteria oceny ofert.
2. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający poinformuje równocześnie Wykonawców, którzy złożyli oferty, przekazując im informacje, o których mowa w art. 253 ust. 1 ustawy Pzp oraz udostępni je na stronie internetowej prowadzonego postępowania www.szpital.sejny.pl
3. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może dokonać ponownego badania i oceny ofert, spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

XIX. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający zawrze umowę w sprawie zamówienia publicznego, w terminie i na zasadach określonych w art. 308 ust. 2 i 3 ustawy Pzp.
2. Zamawiający poinformuje Wykonawcę, któremu zostanie udzielone zamówienie, o miejscu i terminie zawarcia umowy.
3. Przed zawarciem umowy Wykonawca, na wezwanie Zamawiającego, zobowiązany jest do podania wszelkich informacji niezbędnych do wypełnienia treści umowy.
4. W przypadku wyboru oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Wykonawcy ci, na wezwanie Zamawiającego, zobowiązani będą przed zawarciem umowy w sprawie zamówienia publicznego przedłożyć kopię umowy regulującej współpracę tych Wykonawców.
5. Jeżeli Wykonawca nie dopełni ww. formalności w wyznaczonym terminie, Zamawiający uzna, że zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy i będzie upoważniony do zatrzymania wadium na podstawie art. 98 ust. 6 pkt 3 ustawy Pzp.

XX. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie będzie żądał zabezpieczenia należytego wykonania umowy

XXI. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Projekt umowy stanowi załącznik do niniejszej SWZ.
2. Zamawiający dopuszcza możliwość zmian umowy w zakresie i na warunkach określonych zgodnie z załącznikiem do SWZ "Projekt umowy"

XXII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy Pzp,

   Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
2. **Odwołanie przysługuje na:**

2) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy,
3) zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy.

Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.

Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub treści SWZ na stronie internetowej.

Odwołanie wnosi się w terminie:

1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).

Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp,, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.

W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.

Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych, zwanego dalej "sądem zamówień publicznych".

Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy Pzp,, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe jest równoznaczne z jej wniesieniem.

Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.

XXIII. KLAUZULA INFORMACYJNA Z ART. 13 RODO DO ZASTOSOWANIA PRZEZ ZAMAWIAJĄCYCH W CELU ZWIĄZANYM Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest *Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach, adres: ul. E. Rittlera 2, 16-500 Sejny, reprezentowany przez Dyrektora SP ZOZ w Sejnach – Waldemara Kwaterskiego, tel. 87 517 23 17 e-mail: w.kwaterski@szpital.sejny.pl*
- Inspektorem ochrony danych osobowych w *SP ZOZ w Sejnach* jest Pan *Bartosz Wiżlański, tel. 87 517 23 46; e-mail: b.wizlanski@szpital.sejny.pl*
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego;
- 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 2019 r. – Prawo zamówień publicznych, dalej „ustawa Pzp";
- 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;
- 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;

- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - **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.*

XXIV. ZAŁĄCZNIKI DO NINIEJSZEJ SPECYFIKACJI

1. Załącznik nr 1 – Formularz ofertowy.
2. Załącznik nr 2 – Formularz wymaganych parametrów
3. Załącznik nr 3 – Umowa – projekt
4. Załącznik nr 4 – Umowa o zachowaniu poufności z załącznikami
5. Załącznik nr 5 – Oświadczenia Wykonawcy.
6. Załącznik nr 6 – Oświadczenie o przynależności, lub braku przynależności do tej samej grupy kapitałowej.

ZAŁĄCZNIK NR 1

pieczęć firmowa Wykonawcy

.....dnia.....

FORMULARZ OFERTOWY

I. Dane dotyczące Wykonawcy:

	Wypełnia Wykonawca

Pełna nazwa Wykonawcy /firma, , w zależności od podmiotu:	
Adres (ulica, miejscowość, powiat, województwo)	
NIP:	
Regon	
KRS /CEIDG	Działający zgodnie z wpisem do……. prowadzonego przez……. pod numerem KRS/CEIDG ……..(jeżeli dotyczy):
Kapitał zakładowy (jeżeli dotyczy):	
Imię i nazwisko osoby prowadzącej sprawę oraz nr telefonu:	
Nr faksu służbowego, czynnego całą dobę, za pomocą którego zamawiający będzie przysyłał stosowne dokumenty dotyczące przedmiotowego postępowania:	
Kontakt internetowy (strona www., e-mail):	
E-mail służbowy osoby prowadzącej sprawę:	
Numer konta bankowego na, które należy dokonać zapłaty:	

II. Przedmiot oferty:

Oferujemy wykonanie przedmiotu zamówienia, tj. **Zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa, z podziałem na 4 zadania dla SP ZOZ w Sejnach w zakresie (wpisać numer zadania): ……**

Zadanie nr 1
Wartość brutto: ……zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zadanie nr 2
Wartość brutto: ……zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zadanie nr 3
Wartość brutto: ……zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zadanie nr 4
Wartość brutto: ……zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zamówienie wykonamy w następującym terminie (należy zaznaczyć odpowiednie pole):

☐ do 01.12.2022 r. – 0 pkt

☐ do 25.11.2022 r. – 20 pkt

☐ do 20.11.2022 r. – 40 pkt

III. Płatność

Zamawiający przewiduje płatność w terminie 30 dni od daty otrzymania faktury po dostarczeniu i zamontowaniu urządzeń.

IV. Oświadczenia Wykonawcy :
Oświadczamy, że:

1. jestem małym/średnim przedsiębiorstwem (proszę zaznaczyć odpowiednie pole):
   ☐ Tak
   ☐ Nie
   (Zgodnie z zaleceniem Komisji z dnia 6 maja 2003 r. dotyczącym definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36):
   Małe przedsiębiorstwo: *przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EURO.*
   Średnie przedsiębiorstwa: *przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EURO lub roczna suma bilansowa nie przekracza 43 milionów EURO.)*
2. zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia oraz zawartymi w niej warunkami umowy. Nie wnosimy zastrzeżeń co do ich treści i zobowiązujemy się do zawarcia umowy zgodnie z przedstawionymi warunkami, w miejscu i terminie wskazanym przez Zamawiającego oraz do przystąpienia do zgodnej z nimi realizacji zamówienia niezwłocznie po jej podpisaniu.
3. Wybór oferty **nie będzie/ będzie**[1] prowadził do powstania u Zamawiającego obowiązku podatkowego w VAT (ustawa z dnia 09.04.2015 r. o zmianie ustawy o podatku od towarów i usług oraz ustawy Prawo zamówień Publicznych). W przypadku powstania u Zamawiającego obowiązku podatkowego w VAT informacja winna wskazywać: nazwę (rodzaj) usługi, której świadczenie będzie prowadzić do powstania obowiązku podatkowego oraz wartość tej usługi bez kwoty VAT.
4. Oświadczamy, że w przypadku wspólnego ubiegania się o udzielenie zamówienia ponosimy solidarną odpowiedzialność za wykonanie przedmiotu umowy i wniesienie zabezpieczenia należytego wykonania umowy.
5. Wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcy/podwykonawcom:

   ☐ Tak * ☐ Nie

*Jeżeli Wykonawca zamierza powierzyć podwykonawcy części zamówienia i są mu znane nazwy firm podwykonawcy należy wypełnić poniższą tabelę;
W przypadku powierzenia zamówienia podwykonawcy lub podwykonawcom , należy wskazać wartość lub procentową część zamówienia, jaka zostanie powierzona podwykonawcy lub podwykonawcom

części zamówienia przewidzianej do wykonania przez podwykonawcę:
……..
Nazwa/firma podwykonawcy:
…… ……..
Wartość lub procentowa część zamówienia, jaka zostanie powierzona podwykonawcy lub podwykonawcom:…….. ……

6. Oświadczamy, że oferta **nie zawiera/zawiera*** informacji/-e stanowiących/-e tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. W przypadku braku wskazania jednej z opcji Zamawiający przyjmie, że oferta nie zawiera informacji stanowiących tajemnicę przedsiębiorstwa.
7. Oświadczam/y, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO [2)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
8. Oświadczam, że uważam się za związanego niniejszą ofertą na czas określony w specyfikacji istotnych warunków zamówienia.

9. Podane ceny brutto zawierają wszystkie koszty, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.
10. Pod groźbą odpowiedzialności karnej oświadczamy, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień otwarcia ofert (art. 297 K.K.)
11. Oferta wraz z oświadczeniami i dokumentami została złożona na …….. stronach kolejno ponumerowanych od 1 do …… .
12. Osoba upoważniona do koordynowania dostaw z Zamawiającym w przypadku udzielenia nam zamówienia to: ..... nr tel. .....

Integralną część oferty stanowią następujące dokumenty:
1/ .....
2/ .....
3/ .....
4/ .....

……
Miejscowość / Data

……..
Podpis(y) osoby(osób) upoważnionej(ych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów)

[1] Niepotrzebne skreślić
[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

* W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie)

Załącznik nr 2. Formularz wymaganych parametrów.

Zadanie 1

Zakup i wdrożenie kompleksowej platformy systemu kopii bezpieczeństwa

W ramach przedmiotu zamówienia wykonawca zobowiązany jest uruchomić zamówioną kompleksową platformę do wykonywania kopii bezpieczeństwa (autoloader, program do wykonywania backupu, usługa wykonywania kopii zapasowych w chmurze) na zaktualizowanym przez niego środowisku serwerowym Windows Server 2022 (6 serwerów fizycznych, 15 maszyn wirtualnych) zamawiającego. Wykonawca zaktualizuje systemy serwerowe, skonfiguruje dostarczone rozwiązanie na zaktualizowanym środowisku posiadanym przez zamawiającego i uruchomi produkcyjnie system klasy HIS na dostarczonym rozwiązaniu. Wdrożony system kopii zapasowych musi zapewniać bezproblemową pracę po podłączeniu go do sieci informatycznej zamawiającego. Wykonawca jest zobowiązany dokonać instalacji oprogramowania w miejscach wskazanych przez Zamawiającego. Szczegóły dotyczące aktualizacji i instalacji systemu zostaną ustalone w trakcie realizacji projektu. Prace instalacyjne mogą być wykonywane zdalnie.

1.1. Usługa realizowania kopii zapasowej posiadanego przez zamawiającego systemu klasy HIS w chmurze – 1 szt./3 lata

1. Usługa powinna być kierowana do obsługi silnika baz danych Oracle posiadanego przez Zamawiającego.
2. Kopie zapasowe bazy danych w chmurze muszą być zintegrowane z Recovery Manager firmy Oracle.
3. Informacje o kopiach zapasowych w chmurze musza być przechowywane w pliku kontrolnym posiadanej bazy danych oraz w katalogu odzyskiwania.
4. Do tworzenia kopii zapasowych wymagane jest szyfrowanie kopii zapasowych.
5. Oferowana usługa powinna pozwalać na szyfrowanie: hasłem oraz przezroczystym szyfrowaniem danych (TDE).
6. Usługa do transportu backupu musi zapewniać szyfrowanie w locie (in-transit encryption).
7. Uwierzytelnianie do usługi musi odbywać się za pomocą kluczy kryptograficznych.
8. Usługa musi umożliwiać backup baz danych uruchomionych w środowiskach: Windows, Linux i Solaris.
9. Wykonawca musi wykonać konfigurację kopii zapasowej w chmurze dla posiadanego systemu klasy HIS.
10. Kopie zapasowe w chmurze muszą być przechowywane na terenie Unii Europejskiej.
11. Wykonawca zapewni szkolenia z zakresu obsługi dostarczonego rozwiązania dla minimum 2 osób.
12. Usługa świadczona przez 36 miesięcy. Przypisanie licencji na Zamawiającego.
13. W ramach przedmiotu zamówienia wykonawca zobowiązany jest uruchomić oprogramowanie na zaktualizowanym przez niego środowisku serwerowym Windows Server 2022 (6 serwerów fizycznych, 15 maszyn wirtualnych) zamawiającego. Wdrożony system kopii zapasowych musi zapewniać bezproblemową pracę po podłączeniu go do sieci informatycznej zamawiającego. Wykonawca jest zobowiązany dokonać instalacji oprogramowania w miejscach wskazanych przez Zamawiającego. Prace instalacyjne mogą być wykonywane zdalnie.
14. Gwarancja i rękojmia na wykonane instalacje i poprawność tworzenia kopii od momentu podpisania protokołu odbioru przez okres 12 miesięcy.

1.2. Oprogramowanie do wykonywania backupów – 1 szt./20 szt. (środowisko wirtualne)/5 lat

1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: minimalna liczba referencji 150, minimalna ocena z referencji 4,5. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
2. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
3. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
4. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.

5. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
6. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
7. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
8. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
9. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
10. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
11. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
12. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
13. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
14. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
15. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i HyperV używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
16. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
17. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.
18. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
19. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na Vmware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
20. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Vmware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
21. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
22. System musi mieć status „Vmware Ready" i być przetestowany i certyfikowany przez Vmware.
23. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
24. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.

25. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz XLS.
26. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
27. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
28. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
29. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).

30. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
31. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
32. System musi mieć możliwość eksportowania raportów do formatów DOC, XLS, PDF.
33. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
34. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.
35. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.
36. Rozwiązanie musi wspierać systemy operacyjne macOS.
37. Rozwiązanie musi wspierać następujące wersje macOS: Big Sur, Catalina.
38. Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2.
39. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
40. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.
41. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.
42. Rozwiązanie musi wspierać backup podłączonych dysków USB.
43. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
44. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
• Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny,
• Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire,
• Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS,
• Zcentralizowanym repozytorium danych,
•Bezpośrednio na zasobach Chmury.
45. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
46. Rozwiązanie musi wspierać kontrolę pasma sieciowego.
47. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.
48. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.

49. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.
50. Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
51. Rozwiązanie musi wspierać technologię BitLocker.
52. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.
53. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla:
• Microsoft Exchange 2010 i nowszych,
• Microsoft Active Directory 2003 I nowszych,
• Microsoft Sharepoint 2010 i nowszych,
• Microsoft SQL 2005 i nowszych,
• Oracle 11g i nowszych.
54. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
55. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
56. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
57. Rozwiązanie musi wspierać szyfrowanie.
58. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.
59. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.
60. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
61. Powyższa funkcjonalność ma działać w środowisku wirtualnym. Wymagane jest dostarczenie licencji dla zabezpieczenie minimum 20 sztuk wirtualnych i fizycznych serwerów.
62. Wraz z oprogramowaniem wymagane jest dostarczenie wsparcia producenta oprogramowania na okres 60 miesięcy.
63. Usługa świadczona przez 60 miesięcy. Przypisanie licencji na Zamawiającego.
64. W ramach przedmiotu zamówienia wykonawca zobowiązany jest uruchomić oprogramowanie na zaktualizowanym przez niego środowisku serwerowym Windows Server 2022 (6 serwerów fizycznych, 15 maszyn wirtualnych) zamawiającego. Wdrożony system kopii zapasowych musi zapewniać bezproblemową pracę po podłączeniu go do sieci informatycznej zamawiającego. Wykonawca jest zobowiązany dokonać instalacji oprogramowania w miejscach wskazanych przez Zamawiającego. Prace instalacyjne mogą być wykonywane zdalnie.
65. Gwarancja i rękojmia na wykonane instalacje i poprawność tworzenia kopii od momentu podpisania protokołu odbioru przez okres 12 miesięcy.

1.3. Aktualizacja licencji oprogramowania serwerowego wykorzystywanego w jednostce w procesie wykonywania kopii bezpieczeństwa

W ramach przedmiotu zamówienia wykonawca zobowiązany jest uruchomić oprogramowanie Windows Server 2022 (zaktualizować/zainstalować istniejące serwery Windows Server 2012 R2: 6 serwerów fizycznych, 15 maszyn wirtualnych) zamawiającego. Wykonawca zaktualizuje systemy serwerowe, skonfiguruje dostarczone rozwiązanie na zaktualizowanym środowisku posiadanym przez zamawiającego i uruchomi produkcyjnie system klasy HIS na dostarczonym

rozwiązaniu. Zaktualizowane oprogramowanie musi zapewniać bezproblemową pracę istniejących systemów informatycznych zamawiającego i zapewnić bezproblemową pracę w systemach zamawiającego po podłączeniu go do sieci informatycznej zamawiającego. Wykonawca jest zobowiązany dokonać instalacji oprogramowania w miejscach wskazanych przez Zamawiającego. Prace instalacyjne mogą być wykonywane zdalnie.
Gwarancja i rękojmia na poprawne działanie wykonanych instalacji systemów operacyjnych od momentu podpisania protokołu odbioru przez okres 12 miesięcy.

1.3.1. Licencja Microsoft Windows Server Datacenter 2022 – 2 szt.

Funkcjonalność:
- Licencja musi być najnowszą, możliwą do nabycia od producenta
- Licencja nieograniczona czasowo ani funkcjonalnie
- Licencja pozwalająca na uruchomienie nieograniczonej liczby instancji systemów operacyjnych (OSE) i kontenerów Hyper-V w obrębie serwera fizycznego
- Licencje muszą mieć możliwość ich przenoszenia na inne serwery fizyczne
- Licencja musi pozwalać na zalicencjonowanie 2 serwerów fizycznych posiadających po 2 procesory fizyczne o 6 rdzeniach każdy (2xCPU, 6 rdzeni na CPU)
- wersja językowa US (Angielski Stany Zjednoczone)

Kompatybilność:
- Zastosowanie w środowisku Active Directory Zamawiającego przy poziomie funkcjonalności domeny: 2012, 2016, 2019, 2022
- Możliwość aktualizacji kontrolerów domen Active Directory do najnowszych wersji.

Licencja:
- Zarejestrowanie licencji na dane Zamawiającego
- Licencja CSP w modelu dożywotnim
- Dostępność licencji w portalu Microsoft 365 Admin Center
- Ilość licencji – 2 szt.

1.3.2. Licencja Microsoft Windows Server Standard 2022 – 5 szt.

Funkcjonalność:
- Licencja musi być najnowszą, możliwą do nabycia od producenta
- Licencja nieograniczona czasowo ani funkcjonalnie
- Licencje muszą mieć możliwość ich przenoszenia na inne serwery fizyczne
- Licencja musi pozwalać na zalicencjonowanie 4 serwerów fizycznych posiadających po 1 procesorze fizycznym o 8 rdzeniach każdy (1xCPU, 8 rdzeni na CPU) plus 1 przeznaczona na backup
- wersja językowa US (Angielski Stany Zjednoczone)

Kompatybilność:
- Zastosowanie w środowisku Active Directory Zamawiającego przy poziomie funkcjonalności domeny: 2012, 2016, 2019, 2022

Licencja:
- Zarejestrowanie licencji na dane Zamawiającego
- Licencja CSP w modelu dożywotnim
- Dostępność licencji w portalu Microsoft 365 Admin Center
- Ilość licencji – 4 szt.

1.3.3. Windows Server 2022 Device CAL – 150 szt.

- Ilość licencji – 150 szt.
- Zarejestrowanie licencji na dane Zamawiającego

Wartość brutto: …….zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zadanie 2

Zakup i wdrożenie systemu antywirusowego dla stacji roboczych i serwerów - centralnie zarządzanych, system klasy Endpoint Detection and Response (EDR) – 175 szt./3 lata

Wymagania:

Administracja zdalna
1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
17. Rozwiązanie musi informować administratora o nieaktualnych komponentach w tym przynajmniej JAVA i serwer SQL.

Ochrona stacji roboczych
1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11), MacOS 10.15 lub nowszy.
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
21. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
29. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera
1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i

nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
Dodatkowe wymagania dla ochrony serwerów Windows:
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
Dodatkowe wymagania dla ochrony serwerów Linux:
18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Endpoint Detection and Response
1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta.
2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica".
6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
9. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania.
10. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.
11. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
12. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell.

Ochrona urządzeń mobilnych opartych o system Android
1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
a. usunięcie zawartości urządzenia,
b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,
d. uruchomienie sygnału dźwiękowego,
e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
a. nazwę aplikacji,
b. nazwę pakietu,
c. kategorię sklepu Google Play,
d. uprawnienia aplikacji,
e. pochodzenie aplikacji z nieznanego źródła.

Licencja
1. 175 stanowisk/obiektów.
2. Subskrypcja na 3 lata
3. Kontynuacja obecnie zainstalowanego rozwiązania w jednostce lub równoważnego*
* za równoważny Zamawiający uzna oprogramowanie spełniające standardy jakościowe systemu wymagane przez Zamawiającego oraz współpracujące bez zakłóceń z systemami operacyjnymi stacji roboczych Windows 10/11 i serwerów Microsoft Windows Server 2012 R2/2022 posiadanymi przez Zamawiającego. W przypadku zaoferowania systemu równoważnego Zamawiający wymaga zainstalowania i skonfigurowania dostarczonego oprogramowania na wskazanych serwerach i stacjach roboczych zabezpieczanych dotychczas przez oprogramowanie ESET (w tym odinstalowania działającego na tych stacjach oprogramowania ESET). Skonfigurowania zaoferowanego oprogramowania (utworzenie odpowiednich grup komputerów, przypisanie komputerów do poszczególnych grup, zdefiniowania odpowiednich reguł aktualizacji, skanowania. Firewall dla poszczególnych grup komputerów i konsoli zarządzającej zgodnie z wymaganiami Zamawiającego). Przeszkolenia administratorów Zamawiającego 3 osoby z administracji, konfiguracji i instalacji wdrożonego oprogramowania (min. 2 dni po 6 godz. szkolenia). Instalacja i konfiguracja ma przebiegać w sposób niezakłócający pracy użytkowników, stacji roboczych oraz serwerów.
4. Możliwość dokupienia kolejnych licencji w razie potrzeby.
5. W ramach pakietu dostawca przekaże licencje, zainstaluje na wskazanym serwerze oprogramowanie konsoli zarządzającej. Wdroży polityki bezpieczeństwa dla wskazanych grup użytkowników oraz skonfiguruje pozostałe usługi.

Ogólne
1. Wraz z oprogramowaniem wymagane jest dostarczenie wsparcia producenta oprogramowania na okres 60 miesięcy.
2. Usługa świadczona przez 60 miesięcy. Przypisanie licencji na Zamawiającego.
3. W ramach przedmiotu zamówienia wykonawca zobowiązany jest uruchomić oprogramowanie na zaktualizowanym przez niego środowisku serwerowym Windows Server 2022 (6 serwerów fizycznych, 15 maszyn wirtualnych) zamawiającego. Wdrożony system kopii zapasowych musi zapewniać bezproblemową pracę po podłączeniu go do sieci informatycznej zamawiającego. Wykonawca jest zobowiązany dokonać instalacji oprogramowania w miejscach wskazanych przez Zamawiającego. Prace instalacyjne mogą być wykonywane zdalnie.
4. Gwarancja i rękojmia na wykonane instalacje i poprawność działania oprogramowania od momentu podpisania protokołu odbioru przez okres 12 miesięcy.

Wartość brutto: ……zł

Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zadanie 3

Zakup i wdrożenie urządzenia typu Firewall – 1 szt./5 lat

Wymagania Ogólne
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się,aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

- 10 portami Gigabit Ethernet RJ-45 (min. 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port).

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:
W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji, jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona

platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej 5 lat.
3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

5. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na 60 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wsparcie Techniczne

1. Usługa (Aktywne Wsparcie – 20 godzin/rok) obejmuje pomoc w identyfikacji i rozwiązywaniu problemów dotyczących wskazanych elementów infrastruktury informatycznej Klienta, kontaktów z producentem, wykonywanie prac konfiguracyjnych, konsultacje w zakresie integracji wskazanych rozwiązań z innymi elementami infrastruktury IT.

Rozszerzone wsparcie serwisowe

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

Wdrożenie

Wykonawca wykona wdrożenie dostarczonego urządzenia poprzez implementację posiadanych usług sieciowych występujących u Zamawiającego wraz z konfiguracją m.in. VLAN, VPN, IPS/IDS. Wdroży polityki bezpieczeństwa dla wskazanych grup użytkowników oraz skonfiguruje pozostałe usługi.
Gwarancja i rękojmia na wykonane konfiguracje i poprawność działania oprogramowania od momentu podpisania protokołu odbioru przez okres 60 miesięcy.

Wartość brutto: …….zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Zadanie 4

Zakup i wdrożenie biblioteki taśmowej – 1 szt.

1. Przedmiotem zamówienia jest dostarczenie biblioteki taśmowej (autoloader) umożliwiającej przechowywanie danych na nośnikach taśmowych typu LTO-9.
2. Napęd LTO-9 powinien być wyposażony w złącze FC 8Gb. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie także napędów LTO szóstej, siódmej i ósmej generacji. Oferowane urządzenie musi mieć możliwość instalowania i wykorzystania w tej samej obudowie także napędów LTO z interfejsem SAS oraz wspierać technologię LTFS (Linear Tape File System.
3. Prędkość zapisu zainstalowanego napędu bez kompresji – minimum 300 MB/sek.
4. Zainstalowany napęd musi dynamicznie i płynnie dopasowywać prędkość zapisu do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek., oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania dysku oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2.
5. Wymagane jest posiadanie przez urządzenie minimalnie 8 slotów na nośniki podzielone na dwa magazynki. Urządzenie powinno być dostarczone z kompletem magazynków. Wymagana ilość mail slot (I/E) - 1 szt.
6. Pojemność bez kompresji – minimum 144TB.
7. Zarzadzanie odbywa się za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć, poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
8. Biblioteka musi być wyposażone w interfejsy: sieciowy, USB, ADI oraz złącze FC 8Gb.
9. Urządzenie ma mieć możliwość wymiany napędu, zasilacza i modułu portów zarządzania u użytkownika, bez konieczności demontażu urządzenia z szafy RACK i bez konieczności zdejmowania pokrywy głównej. Zarówno napęd, jak i moduł interfejsów powinny być wyposażone w lampki kontrolne, informujące o stanie technicznym.
10. Obudowa typu rack 19” o wysokości maksymalnie 1U. Wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem.
11. Urządzenie musi być wyposażone w czytnik kodów kreskowych, kabel zasilający oraz zestaw 8-miu nośników danych o pojemności bez kompresji (minimum 18 TB każdy) wraz z nośnikiem czyszczącym, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem oraz wyposażone w naklejki z kodami kreskowymi.
12. Gwarancja - 36 miesięcy w miejscu instalacji urządzenia z czasem reakcji w ciągu 4 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszania awarii wyłącznie poprzez

ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim.

13. Pisemne oświadczenia wystawione przez producenta:
    - o gwarancji świadczonej w miejscu instalacji urządzenia w rygorze 24x7x4 realizowanej przez producenta lub jego autoryzowany serwis posiadający ISO9001 na usługi serwisowe wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy. W oświadczeniu wymagane jest podanie wszystkich danych kontaktowych z serwisem (mail, telefon, adres) oraz potwierdzenie wykupienia przez wykonawcę wymienionych usług serwisowych u producenta.
    -- o oferowaniu urządzenia zgodnego z zapisami specyfikacji technicznej przetargu oraz europejskimi normami dotyczącymi CE i WEEE – oświadczenie musi być podpisane i wystawione nie wcześniej niż 1 miesiąc przed ogłoszeniem postępowania przetargowego.
14. Wykonawca dostarczy, zamontuje i poprawnie skonfiguruje bibliotekę taśmową.
15. 1Wykonawca dostarczy, zamontuje i poprawnie skonfiguruje kartę FC HBA w posiadanym serwerze Fujitsu Siemens PRIMERGY RX2540M1R4 celem połączenia z autoloaderem.
16. Gwarancja i rękojmia na wykonane instalacje i części od momentu podpisania protokołu odbioru przez okres 36 miesięcy.

Wartość brutto: …….zł
Podatek Vat: …….. % ……..zł
Wartość netto: ..…… zł

Załącznik nr 3

Umowa – projekt

Umowa jest wynikiem przeprowadzonego postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie art. 275 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U. 2022.poz. 1710 ze zm.) zwana dalej Pzp lub ustawą

Zawarta dnia …… 2022 r. w Sejnach pomiędzy:

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej z siedzibą w Sejnach, ul. Dr. Edwarda Rittlera 2, 16-500 Sejny, wpisanym do Krajowego Rejestru Sądowego pod numerem KRS 0000016297, numer REGON 790317340, numer NIP 844-17-84-785, **reprezentowanym ……..**, zwanym dalej jako „**Zamawiający**”,
a

……
…….., zwanego dalej jako „**Wykonawca**”,

łącznie zwanymi „**Stronami**”, a pojedynczo „**Stroną**”, o następującej treści:

§1.

1. Przedmiotem umowy jest podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Sejnach poprzez realizację zadania nr …….. zgodnie ze złożoną ofertą z dnia ……. r. stanowiącą **załącznik** do niniejszej umowy.
2. Szczegółowy opis przedmiotu zamówienia określony został w **załączniku nr 1** do specyfikacji warunków zamówienia, stanowiącym **załącznik nr 1** i integralną część niniejszej umowy.

§2.

Wykonawca wykona Przedmiot Umowy określony w §1 w terminie nieprzekraczalnym terminie do dnia …… 2022 r.

§3.

1. Strony ustalają, że za wykonanie przedmiotu umowy Zamawiający zapłaci wynagrodzenie ustalone na podstawie złożonej oferty przelewem na rachunek bankowy Wykonawcy.
2. Zamawiający zobowiązuje się do zapłaty za przedmiot umowy na podstawie faktury wystawionej przez Wykonawcę, przelewem w terminie do ……dni od dnia otrzymania faktury.
3. Podstawą do wystawienia przez Wykonawcę faktury będzie Protokół odbioru podpisany przez Zamawiającego bez zastrzeżeń.
4. Za dzień zapłaty Strony uznają dzień obciążenia rachunku bankowego Zamawiającego.
5. Zamawiający na podstawie art. 106n ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług udziela Wykonawcy zgody na wystawianie i przesyłanie z adresu e-mail: _____ faktur, duplikatów faktur oraz ich korekt, a także not obciążeniowych i not korygujących w formacie pliku elektronicznego PDF na adres e-mail ……..

§4.

1. Wykonawca oświadcza, że dysponuje odpowiednim potencjałem techniczno–organizacyjnym, personelem posiadającym odpowiednie kwalifikacje oraz wiedzę i doświadczenie pozwalające na należytą realizację przedmiotu Umowy.
2. Wykonawca zapewni Zespół specjalistów posiadających kwalifikacje, wiedzę i doświadczenie dedykowane do realizacji Umowy.
3. W zależności od wykonywanych prac zostanie przydzielony użytkownik i hasło z uprawnieniami wynikającymi z polityki bezpieczeństwa.
4. Osobami uprawnionymi do bieżących kontaktów w ramach realizacji przedmiotu umowy oraz do odbioru Raportu i podpisywania protokołów są osoby:
   1) po stronie Zamawiającego: Pan/i _____e-mail: _____
   2) po stronie Wykonawcy: Pan/i _____ e-mail: _____

§5.

1. Zamawiający zobowiązuje się do współdziałania z Wykonawcą, w szczególności poprzez:
   1) współpracę w zakresie planowania przez Wykonawcę czynności w zakresie realizacji przedmiotu Umowy,
   2) umożliwienie Wykonawcy wykonania przedmiotu Umowy określonego w §1 ust. 1 Umowy.
2. Strony zgodnie ustalają, że na potrzeby realizacji Umowy do wymiany korespondencji będą używać drogi elektronicznej w postaci przesyłania wiadomości e-mail opatrzonych każdorazowo imieniem i nazwiskiem osoby wysyłającej wiadomość bez konieczności podpisywania korespondencji kwalifikowanym podpisem elektronicznym. Na potrzeby realizacji Umowy Strony udostępniają adresy e-mail określone w §4 ust. 8. Strony gwarantują, że powyższymi adresami posługiwać się mogą wyłącznie osoby upoważnione do kontaktów z drugą Stroną.
3. Wykonawca gwarantuje, że jego usługi będą świadczone w profesjonalny sposób, według odpowiedniej wiedzy i doświadczenia, z najwyższą starannością i efektywnością, oraz że wykona zlecone mu prace terminowo i zgodnie i obowiązującym stanem prawnym.
4. Wykonawca uprawniony będzie do realizacji Przedmiotu Umowy w siedzibie Zamawiającego lub zdalnie po uzyskaniu pisemnej zgody Zamawiającego.
5. Wykonawca dołoży wszelkich starań w celu uniknięcia wpływu testów na prace testowanych systemów. Termin i zakres prowadzenia prac będzie każdorazowo uzgadniany z Zamawiającym, tak aby zminimalizować potencjalne skutki testów.
6. Wykonawca ponosi całkowitą odpowiedzialność za swoje działania lub zaniechania związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy Zamawiającego lub osoby trzeciej za którą Wykonawca nie ponosi odpowiedzialności.
7. Wykonawca nie jest uprawniony do wprowadzania jakichkolwiek zmian do systemów teleinformatycznych Zamawiającego bez pisemnej zgody Zamawiającego, w szczególności Wykonawca zobowiązuje się nie wprowadzać żadnych zmian do baz danych wykorzystywanych przez Zamawiającego.
8. Zawierając Umowę Wykonawca zobowiązuje się jednocześnie do zawarcia z Zamawiającym umowy o zachowaniu poufności, której projekt wraz z załącznikami stanowi **Załącznik nr 4** do Umowy.

§6.

1. Wykonawca przekazuje Zamawiającemu informację o zakończeniu zadania wraz z dołączonym protokołem odbioru na wskazany w Umowie adres mailowy.
2. Zamawiający w terminie do 3 dni roboczych zaakceptuje przekazane informacje albo zgłosi uwagi, przesyłając je na adres określony w §4 ust. 8 pkt 2).
3. W przypadku zgłoszenia uwag przez przedstawicieli Zamawiającego wskazanych w §4 ust. 8 pkt 1), Wykonawca odpowie na zgłoszone przez Zamawiającego uwagi i w przypadku uwzględnienia uwag

Zamawiającego ponownie przedstawi Zamawiającemu do akceptacji poprawione informacje, nie później niż w terminie 5 dni roboczych od otrzymania uwag od Zamawiającego.
4. W przypadku zgłoszenia przez Zamawiającego dalszych uwag do wykonania przedmiotu Umowy, postanowienia ust. 3 i 4 stosuje się odpowiednio.
5. Odbiór zadania nastąpi w formie Protokołu odbioru, podpisanego przez Zamawiającego bez zastrzeżeń.
6. Za termin wykonania przedmiotu umowy strony uznają dzień podpisania przez Zamawiającego protokołu odbioru bez zastrzeżeń.

§7.

Wykonawca udziela gwarancji i rękojmi zgodnie z załącznikami do umowy.

§8.

Strony ustalają, że w razie niewykonania lub nienależytego wykonania umowy obowiązywać będą kary umowne.

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   - 5% wartości zamówienia netto gdy Zamawiający odstąpi od umowy z powodu okoliczności, za które odpowiada Wykonawca.
   - 2% wartości umowy netto za każdy dzień zwłoki w dostawie po planowanym terminie dostawy.
2. Zamawiający zapłaci Wykonawcy kary umowne:
   - 5% wartości zamówienia netto za odstąpienie od umowy z przyczyn leżących po jego stronie.

3. Wykonawca wyraża zgodę na potrącenie kar umownych z należnego mu wynagrodzenia.
4. Łączna wysokość kar umownych nie może przekroczyć 50% wartości zamówienia netto.
5. Strony zastrzegają możliwość dochodzenia odszkodowania przenoszącego wartość kar umownych na zasadach ogólnych.

§9.

1. Zamawiającemu przysługuje prawo do odstąpienia od umowy w przypadku gdy Wykonawca nie rozpoczął realizacji umowy lub nie kontynuuje jej niezwłocznie po wezwaniu złożonym na piśmie przez Zamawiającego.
2. Zamawiającemu przysługuje prawo do wypowiedzenia umowy w trybie natychmiastowym, bez zachowania okresu wypowiedzenia w następujących przypadkach:
   1) w przypadku niewykonania lub nienależytego wykonywania przedmiotu umowy przez Wykonawcę w terminie określonym w umowie– w takim wypadku Zamawiający wyznaczy Wykonawcy dodatkowy 5-dniowy termin na wykonanie zobowiązania. Jeśli Wykonawca nie wykona przedmiotu umowy w sposób należyty w tym terminie, Zamawiający ma prawo wypowiedzieć umowę ze skutkiem na dzień złożenia wypowiedzenia,
   2) naruszył bezpieczeństwo informacji lub zasady z nim związane.
3. Oświadczenie o odstąpieniu lub wypowiedzeniu powinno być złożone na piśmie i zostać dostarczone drugiej Stronie.
4. Odstąpienie od umowy nie wpływa na obowiązek zachowania poufności informacji.

7. Siła wyższa:
   1) Żadna Strona nie będzie odpowiedzialna za niewykonanie swoich zobowiązań w ramach umowy w stopniu, w jakim opóźnienie w jej działaniu lub inne niewykonanie jej zobowiązań jest wynikiem Siły Wyższej,
   2) Dla potrzeb umowy „Siła Wyższa" oznacza wydarzenie nadzwyczajne pozostające poza kontrolą Strony, występujące po podpisaniu umowy przez obie Strony, przeszkadzające racjonalnemu wykonaniu przez tę Stronę jej obowiązków, (nie obejmujące winy własnej lub nienależytej staranności tej Strony) i nieprzewidywalne w dacie zawarcia umowy.
   3) Jeżeli Siła Wyższa spowoduje niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy:
      a) Strona – o ile będzie to możliwe - zawiadomi w terminie 2 dni na piśmie drugą Stronę o powstaniu i zakończeniu tego zdarzenia, w miarę możliwości przedstawiając stosowną dokumentację w tym zakresie,
      b) Strona niezwłocznie przystąpi do dalszego wykonywania umowy,
      c) Strony uzgodnią sposób postępowania wobec tego zdarzenia oraz terminy wykonywania umowy.
   4) Jeżeli Siła Wyższa spowoduje niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy przez okres powyżej trzech tygodni, Strony spotkają się i w dobrej wierze rozpatrzą celowość i warunki rozwiązania umowy.

§10.

Ewentualne spory wynikłe na tle realizacji Umowy Strony będą starały się załatwiać polubownie. W przypadku braku porozumienia sądem właściwym miejscowo do rozstrzygania sporów będzie sąd właściwy dla siedziby Zamawiającego.

§11.

1. Informacją w rozumieniu Umowy są wszelkie informacje, dokumenty lub dane przekazane Wykonawcy przez Zamawiającego, uzyskane przez Wykonawcę w związku z realizacją Umowy oraz wytworzone przez Wykonawcę na potrzeby realizacji Umowy.
2. Wykonawca może przetwarzać powierzone mu przez Zamawiającego informacje przez okres obowiązywania Umowy.
3. Wykonawca zobowiązuje się po zakończeniu realizacji Umowy do zwrotu Zamawiającemu wszelkich udostępnionych oraz wytworzonych przez siebie w związku z realizacją Umowy informacji, wraz z nośnikami. W przypadku utrwalenia na nośnikach należących do Wykonawcy informacji uzyskanych w związku z realizacją Umowy, Wykonawca zobowiązuje się do usunięcia z nośników tych informacji, w tym również sporządzonych kopii zapasowych, oraz zniszczenia wszelkich danych, dokumentów mogących posłużyć do odtworzenia, w całości lub części, informacji.
4. Wykonawca zobowiązuje się do przestrzegania wytycznych Zamawiającego o ochronie udostępnianych informacji.
5. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji, a także sposobów zabezpieczenia informacji, zarówno w trakcie trwania niniejszej Umowy, jak i po jej wygaśnięciu lub rozwiązaniu. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez osoby realizujące Umowę.
6. Wykonawca zobowiązany jest do zastosowania wszelkich niezbędnych środków technicznych i organizacyjnych zapewniających ochronę przetwarzania informacji, a w szczególności powinien zabezpieczyć informacje przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem postanowień Umowy, zmianą, utratą, uszkodzeniem, zniszczeniem lub kradzieżą.
7. Wykonawca zobowiązuje się do dołożenia najwyższej staranności w celu zabezpieczenia informacji przed bezprawnym dostępem, rozpowszechnianiem lub przekazaniem osobom trzecim.
8. Wykonawca zobowiązany jest zapewnić wykonanie obowiązków w zakresie bezpieczeństwa informacji, w szczególności dotyczącego zachowania w tajemnicy informacji, także przez jego pracowników oraz osoby, które realizują Umowę w imieniu Wykonawcy. Odpowiedzialność za naruszenie powyższego obowiązku spoczywa na Wykonawcy. Naruszenie bezpieczeństwa informacji, w szczególności ujawnienie jakiejkolwiek informacji w okresie obowiązywania Umowy, uprawnia do odstąpienia przez Zamawiającego od Umowy.
9. Wykonawca może udostępniać informacje jedynie tym swoim pracownikom lub osobom współpracującym na podstawie umów cywilnoprawnych, którym będą one niezbędne do wykonania powierzonych im czynności i tylko w zakresie, w jakim muszą mieć do nich dostęp dla celów określonych w niniejszej Umowie.
10. Wykonawca oraz inne osoby, które realizują Umowę w imieniu Wykonawcy, zobowiązane są przed przystąpieniem do prac do podpisania oświadczenia o zachowaniu poufności informacji. Podpisane oświadczenie należy przekazać Zamawiającemu przed rozpoczęciem realizacji Umowy przez ww. pracowników.
11. Wykonawca ponosi wszelką odpowiedzialność, tak wobec osób trzecich, jak i wobec Zamawiającego, za szkody powstałe w związku z nienależytą realizacją obowiązków dotyczących zapewnienia bezpieczeństwa informacji.
12. Wykonawca zobowiązuje się do ścisłego przestrzegania warunków niniejszej Umowy, które wiążą się z ochroną informacji, w szczególności nie może bez pisemnego upoważnienia Zamawiającego wykorzystywać informacji w celach niezwiązanych z realizacją Umowy.
13. W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji lub z naruszeniem obowiązków wynikających z Umowy, Zamawiający może przeprowadzić kontrolę wykonywanych przez Wykonawcę czynności. Kontrola może być realizowana przez Zamawiającego lub podmioty przez niego uprawnione. Wykonawca zobowiązany jest współpracować z Zamawiającym w odpowiednim zakresie z podmiotami przeprowadzającymi kontrolę. Wyniki kontroli zostaną przekazane Wykonawcy po jej zakończeniu. Zamawiający może wskazać niezbędne działania, jakie Wykonawca musi podjąć w celu wprowadzenia określonych zmian lub podjęcia określonych czynności.
14. Wykonawca zobowiązany jest do natychmiastowego powiadamiania o nieuprawnionym ujawnieniu lub udostępnieniu informacji oraz o innym naruszeniu bezpieczeństwa informacji, a następnie raportowania Zamawiającemu o podjętych działaniach w powyższym zakresie:
    1) telefonicznie, na numer telefonu: _____ .
    2) na adres email: _____ .
    Powiadomienie dokonane telefonicznie musi zostać potwierdzone poprzez sposób wskazany w pkt 2) w terminie jednej godziny od dokonania powiadomienia.
15. Wykonawca nie może zwielokrotniać, rozpowszechniać, korzystać w celach niezwiązanych z realizacją Umowy oraz ujawniać informacji osobom trzecim, bez uzyskania w powyższym zakresie pisemnej

zgody Zamawiającego, o ile takie informacje nie zostały już podane do publicznej wiadomości lub nie są publicznie dostępne.

16. Wykonawca zobowiązany jest:
    1) zapewnić kontrolę nad tym, jakie informacje, kiedy, przez kogo oraz komu są przekazywane;
    2) zapewnić, aby osoby, o których mowa w pkt 1, zachowywały w tajemnicy informacje oraz sposoby ich zabezpieczeń.
17. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji uzyskanych przez niego w związku z zawarciem Umowy. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez podmioty, przy pomocy których wykonuje Umowę.
18. Wykonawca zobowiązany jest zapewnić bezpieczeństwo informacji przed wystąpieniem zagrożeń, w szczególności poprzez:
    1) zastosowanie firewall oraz oprogramowania antyspamowego i antywirusowego,
    2) zapewnienie kontroli dostępu do powierzonych zasobów Zamawiającego,
    3) uniemożliwienie dostępu do haseł do zasobów informatycznych Zamawiającego przez osoby nieuprawnione wraz z ich cykliczną zmianą,
    4) zastosowanie zabezpieczeń ochrony fizycznej.

§12.

1. O ile Umowa nie stanowi inaczej, zmiany treści Umowy mogą być dokonywane wyłącznie w formie aneksu podpisanego przez obie Strony, pod rygorem nieważności w zakresie:
    1) zmiany szczegółowych zasad wykonywania przedmiotu Umowy określonych w załącznikach do Umowy, spowodowane zmianami organizacyjnymi u Zamawiającego;
    2) zmiany zakresu realizacji Przedmiotu Umowy, w przypadku wystąpienia zmiany okoliczności powodującej, że:
        a) realizacja części Przedmiotu Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawierania Umowy,
        b) realizacja części Przedmiotu Umowy nie jest zasadna na skutek zmiany lub planowanej zmiany powszechnie obowiązujących przepisów prawa.
    3) zmiany postanowień Umowy będące następstwem zmian powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy i z których treści wynika konieczność lub zasadność wprowadzenia zmian postanowień Umowy; powyższa zmiana dotyczy także zmiany postanowień Umowy w związku ze zmianą przepisów dotyczących ochrony danych osobowych, w szczególności w zakresie obowiązku spełniania przez Wykonawcę wymagań określonych przez Zamawiającego, poddania się kontroli oraz odstąpienia od Umowy przez Zamawiającego w związku z nieprzestrzeganiem przez Wykonawcę obowiązków związanych z ochroną danych osobowych lub poddaniu się kontroli;
    4) zmiany terminu wykonania Umowy spowodowane zmianą powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy;
    5) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest konieczna w celu prawidłowego wykonania Przedmiotu Umowy;
    6) niezbędna jest zmiana terminu realizacji Umowy w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które obie Strony nie miały wpływu. W takim przypadku termin realizacji umowy zostanie odpowiednio wydłużony o czas trwania przyczyny uniemożliwiającej realizację Umowy;
2. Zmiany, o których mowa w ust. 1 pkt 1 - 6, nie mogą spowodować zwiększenia łącznego wynagrodzenia brutto, o którym mowa w §3 ust. 1.

§13.

1. Wszelkie zmiany i uzupełnienia Umowy, jej wypowiedzenie, rozwiązanie za zgodą obu Stron lub odstąpienie od niej dokonywane będą w formie pisemnej pod rygorem nieważności.
2. Wykonawca bez zgody podmiotu tworzącego Zamawiającego nie może dokonać cesji wierzytelności.
3. Dla potrzeb Umowy Strony ustalają, że ilekroć w umowie jest mowa o dniach roboczych należy przez to rozumieć dni tygodnia przypadające od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
4. W trakcie wykonania przedmiotu Umowy Wykonawca będzie odpowiadać jak za swoje własne czyny za wszelkie czyny lub zaniechania swoich pracowników lub innych osób, którym Wykonawca powierzy za zgodą Zamawiającego wykonanie czynności związanych z realizacją Przedmiotu Umowy.
5. Niewykonanie przez Zamawiającego któregokolwiek z uprawnień przysługujących mu na podstawie Umowy nie może w żadnym razie być uważane za zrzeczenie się tego uprawnienia, ani zrzeczenie się innych uprawnień wynikających z postanowień Umowy.

6. Umowę sporządzono w 3 jednobrzmiących egzemplarzach: jeden dla Wykonawcy i dwa dla Zamawiającego.
7. Załączniki do Umowy stanowią integralną część Umowy.

Załączniki do umowy:
Załącznik nr 1 – Formularz wymaganych parametrów,
Załącznik nr 2 – Oferta Wykonawcy.

WYKONAWCA ZAMAWIAJĄCY

Załącznik nr 4

UMOWA O ZACHOWANIU POUFNOŚCI

zawarta w dniu ……. 2022 r. w Sejnach pomiędzy:

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Sejnach z siedzibą w Sejnach, ul. Edwarda Rittlera 2, posiadającym numer NIP 844-17-84-785, R E G O N 790317340 reprezentowanym przez:

…….

zwanym dalej **Zamawiającym**

a

_____

_____

NIP
REGON

zwanym/zwaną dalej **Wykonawcą**

Zamawiający i Wykonawca będą również nazywani osobno **„Stroną”**, a łącznie **„Stronami”.**

W związku z zawarciem w dniu …….. 2022 r. umowy, której przedmiotem jest ……, zwanej dalej „umową podstawową” Strony, w celu właściwej ochrony danych poufnych udostępnianych w trakcie realizacji umowy podstawowej postanawiają, co następuje:

§ 1.

Ilekroć w umowie użyte zostają wyrazy **„Informacje Poufne”** oznaczają one:

1. przekazywane oraz udostępniane Wykonawcy wszelkie informacje lub dane, niezależnie od formy (ustnie, na piśmie lub w jakikolwiek inny sposób) dotyczące w szczególności konfiguracji urządzeń, spraw, planów działalności lub przedsięwzięć Zamawiającego związanych z realizacją lub przedmiotem umowy podstawowej,
2. wszelkie wiadomości związane z działalnością Zamawiającego, w tym informacje techniczne, technologiczne, ekonomiczne, finansowe, handlowe, marketingowe, prawne, organizacyjne przedsiębiorstwa i organizacji pracy,
3. informacje dotyczące organizacji świadczenia usług, sposobu prowadzenia działalności usługowej, używanych programów komputerowych, infrastruktury technicznej i informatycznej, cen usług i cenników,
4. umowy, korespondencja, specyfikacja usług, oferty, zapytania ofertowe, dane kontrahentów (w tym informacje adresowe, dane finansowe, informacje dotyczące zapotrzebowania na usługi),
5. informacje osobowe, w tym informacje o pracownikach oraz współpracownikach Zamawiającego,
6. dane osobowe zwykłe i szczególnej kategorii dotyczące pacjentów Zamawiającego podlegające szczególnej ochronie,

7. wszelkie rozmowy prowadzone pomiędzy przedstawicielami Stron, w związku z realizacją umowy podstawowej oraz informacje przekazywane w ich trakcie przez Zamawiającego.

§ 2.

1. Z uwagi na udostępnianie Informacji Poufnych Wykonawca zobowiązuje się do:
   1) zachowania w tajemnicy wszystkich Informacji Poufnych, niezależnie od formy w jakiej zostały mu przekazane,
   2) niewykorzystywania do celów innych, niż wykonywanie umowy podstawowej Informacji Poufnych, do których dostęp posiadać będzie Wykonawca, w związku z realizacją umowy podstawowej,
   3) zapewnienia odpowiedniego i bezpiecznego sposobu przechowywania wszystkich Informacji Poufnych, do których dostęp posiadać będzie Wykonawca, w związku z realizacją umowy podstawowej w czasie, gdy znajdują się one w posiadaniu Wykonawcy,
   4) zapewnienia dostępu do Informacji Poufnych wyłącznie osobom biorącym udział w realizacji umowy podstawowej ze strony Wykonawcy, którym dostęp ten jest niezbędny do prawidłowej realizacji umowy podstawowej,
   5) poinformowania wszystkich osób uczestniczących w realizacji umowy podstawowej ze strony Wykonawcy o poufnym charakterze udostępnianych i przekazywanych informacji, pouczenia w sprawie ich traktowania jako poufnych oraz odebrania od tych osób oświadczenia wskazanego w § 2 ust. 4 umowy o zachowaniu poufności,
   6) niekopiowania, niepowielania ani niezwielokrotniania Informacji Poufnych w jakikolwiek sposób, chyba że wcześniej w sposób wyraźny zostanie udzielona w formie pisemnej, pod rygorem nieważności, zgoda Zamawiającego na taką czynność i dokonanie czynności jest niezbędne w związku z realizacją umowy podstawowej; Zamawiający zobowiązuje się do zapewnienia dostępu do Informacji Poufnych na potrzeby realizacji umowy osobom biorącym udział w realizacji umowy podstawowej ze strony Wykonawcy, które okażą Zamawiającemu upoważnienie do udziału w realizacji umowy podstawowej,
   7) na pisemny wniosek Zamawiającego, a w przypadku zakończenia realizacji umowy podstawowej, bez konieczności składania przez Zamawiającego pisemnego wniosku, Wykonawca zobowiązany jest do:
      a) niezwłocznego, ale w okresie nie dłuższym niż 5 dni, zwrócenia na własny koszt wszelkich materiałów zawierających jakiekolwiek Informacje Poufne Zamawiającego, wraz ze wszystkimi kopiami, będącymi w jego posiadaniu;
      b) niezwłocznego, ale w okresie nie dłuższym niż 5 dni, zniszczenia, trwałego usunięcia z pamięci masowych Wykonawcy, na własny koszt danych zawierających jakiekolwiek Informacje Poufne, w sposób uniemożliwiający ich odzyskanie.
2. W przypadku naruszenia przez Wykonawcę obowiązków dotyczących Informacji Poufnych, o których mowa w niniejszej umowie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 200 000,00 zł *(słownie: dwieście tysięcy złotych 00/100*) za każde naruszenie.
3. Zamawiający zastrzega sobie prawo do dochodzenia, na zasadach ogólnych, odszkodowania w wysokości przewyższającej karę umowną w przypadku, gdy szkoda poniesiona przez Zamawiającego przekracza wysokość kary umownej, o której mowa w ust. 2.
4. Osoby biorące udział – z ramienia Wykonawcy - w realizacji umowy o zachowaniu poufności, zostaną upoważnione przez niego do realizacji umowy podstawowej, według wzoru stanowiącego załącznik nr 1 do niniejszej umowy oraz złożą oświadczenie zobowiązujące ich do zachowania w tajemnicy Informacji Poufnych według wzoru określonego w załączniku nr 2 do niniejszej umowy, które Wykonawca przekaże Zamawiającemu przed rozpoczęciem wykonywania przedmiotu umowy podstawowej przez poszczególne osoby.
5. Klauzula informacyjna dotycząca przetwarzania przez Zamawiającego danych osobowych stanowi załącznik nr 3 do niniejszej umowy.

§ 3.

1. Zobowiązania określone w § 2 nie mają zastosowania do Informacji Poufnych:
   1) które są w dniu ujawnienia publicznie znane,
   2) których ujawnienie wymagane jest od Wykonawcy na mocy przepisów prawa.
2. Jeżeli Wykonawca zostanie zobowiązany na mocy prawa lub wezwania sądu do ujawnienia jakichkolwiek Informacji Poufnych, niezwłocznie zawiadomi na piśmie Zamawiającego przed dokonaniem ujawnienia.
3. Wykonawca zobowiązany na mocy prawa lub wezwania sądu do ujawnienia Informacji Poufnych, będzie uprawniony do ujawnienia Informacji Poufnej wyłącznie w zakresie wymaganym prawem

oraz zobowiązany do podjęcia wszelkich uzasadnionych środków, mających na celu upewnienie się, że Informacje Poufne są traktowane jako poufne.

§ 4.

Wykonawca ponosi odpowiedzialność za przestrzeganie postanowień niniejszej umowy przez swoich pracowników oraz inne osoby, które będą zaangażowane w proces realizacji umowy.

§ 5.

Niniejsza umowa zostaje zawarta na okres obowiązywania umowy podstawowej, z tym że zobowiązanie do zachowania tajemnicy i poufności Informacji Poufnych i odpowiedzialność z tego tytułu, pozostają w mocy także po wygaśnięciu niniejszej umowy oraz umowy podstawowej.

§ 6.

Wykonawca potwierdza i wyraża zgodę na to, że nie będzie uprawniony do nabycia żadnych praw do Informacji Poufnych przekazanych przez Zamawiającego lub od niego uzyskanych.

§ 7.

1. Wszelkie spory wynikające z niniejszej Umowy będą rozstrzygane przez sąd powszechny właściwy dla rozstrzygania sporów wynikłych z realizacji umowy podstawowej.
2. Do kwestii nieuregulowanych w niniejszej umowie znajdują zastosowanie w przepisy kodeksu cywilnego oraz inne obowiązujące przepisy prawne.

§ 8.

Zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 9.

Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego i jeden egzemplarz dla Wykonawcy.

WYKONAWCA ***ZAMAWIAJĄCY***

_____ _____

załącznik nr 1 do umowy
o zachowaniu poufności

_____

imię i nazwisko

_____

rodzaj i nr dokumentu tożsamości

UPOWAŻNIENIE

Działając w imieniu Wykonawcy …… *(oznaczenie Wykonawcy*), w wykonaniu postanowień § 2 ust. 4 umowy o zachowaniu poufności upoważniam *Panią/Pana* ……..... do udziału w realizacji przedmiotu umowy z dnia ……..….. 2022 r. w zakresie Zadania nr …..

Miejscowość ....., dnia .....2022 r.

…….
czytelny podpis

załącznik nr 2 do umowy
o zachowaniu poufności

…….
(imię i nazwisko)
…….
(adres zamieszkania)
…….
(nazwa i nr dokumentu tożsamości)
……
(nr PESEL)

OŚWIADCZENIE
o zobowiązaniu do zachowania poufności

Ja niżej podpisany(a), reprezentując w dniu/w okresie …….. Wykonawcę / będąc pracownikiem Wykonawcy* podczas realizacji umowy z dnia …… 2022 r. w zakresie Zadania nr ….., z uwagi na udostępnienie Informacji Poufnych, zobowiązuję się do:

1) zachowania w tajemnicy wszystkich Informacji Poufnych uzyskanych podczas realizacji umowy podstawowej, niezależnie od formy i sposobu ich uzyskania,
2) wykorzystania Informacji Poufnych uzyskanych podczas realizacji umowy podstawowej wyłącznie w celu realizacji umowy podstawowej.

Obowiązek zachowania poufności pozostaje w mocy także po zakończeniu wykonywania wyżej wymienionej umowy podstawowej, przez okres 3 lat od zakończenia jej realizacji przez Wykonawcę.

Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w niniejszym oświadczeniu przez SP ZOZ w Sejnach na potrzeby związane z realizacją niniejszej umowy i umowy podstawowej.

**niewłaściwe skreślić*

Miejscowość ....., dnia ..... 2022 r.

…….
czytelny podpis

załącznik nr 3 do umowy o zachowaniu poufności

Szanowni Państwo,

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informujemy, iż:

• ***Administratorem*** *Państwa danych osobowych jest Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach, adres: ul. E. Rittlera 2, 16-500 Sejny, reprezentowany przez Dyrektora SP ZOZ w Sejnach –* ***Waldemara Kwaterskiego****, tel. 87 517 23 17; e-mail: w.kwaterski@szpital.sejny.pl*
• ***Inspektorem Ochrony Danych*** *Osobowych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Sejnach jest Bartosz Wiżlański, tel. 87 517 23 46; e-mail: b.wizlanski@szpital.sejny.pl*
• ***Celem przetwarzania danych osobowych jest:***
- realizacja umowy o w zakresie Zadania nr……,
- prowadzenie rozrachunków i rozliczeń z tytułu realizacji umowy,
- prowadzenie i przechowywanie dokumentacji powstałej w związku z realizacją umowy podstawowej,
• ***Podstawa prawna przetwarzania danych osobowych*** *wynika w szczególności z:*
- art. 6 ust 1 pkt a/ b/c Ogólnego Rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
- Ustawy z dnia 29 września 1994 r. o rachunkowości
- Ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych
• ***Odbiorcą Państwa danych osobowych będą*** *– Dane osobowe Kontrahentów mogą być udostępnione podmiotom upoważnionym na podstawie przepisów prawa;*
• ***Państwa dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej na podstawie*** *– nie dotyczy;*
• ***Państwa dane osobowe będą przechowywane przez*** *okres: zgodnie z ustawą o rachunkowości przez okres 5 lat od rozwiązania umowy (art. 74 ust. 2 pkt. 4)*
• ***Przysługujące Państwu prawa to m.in.:***
- prawo dostępu do treści swoich danych oraz ich poprawiania;
- prawo do sprostowania swoich danych,
• Mają Państwo prawo wniesienia skargi do organu nadzorczego gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
• Podanie Państwa danych osobowych jest dobrowolne, ale niezbędne dla realizacji wymienionych celów zbierania danych;
• Przetwarzanie podanych przez Panią/Pana danych osobowych nie będzie podlegało zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO.

…….
czytelny podpis

Załącznik nr 5 do SWZ

Wykonawca: …….

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

reprezentowany przez:

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

.....dnia.....

Oświadczenie Wykonawcy

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

Prawo zamówień publicznych dotyczące podstaw wykluczenia z postępowania

Na potrzeby postępowania o udzielenie zamówienia publicznego:

……
(wpisać nazwę Zadania)
prowadzonego przez Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach, oświadczam/my, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.

…….……. *(miejscowość),* dnia …….……. r.

……
(podpis)

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, 5 lub 6 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:

……

…….……. *(miejscowość),* dnia ……. r.

……
(podpis)

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.

Oświadczenie Wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.
Prawo zamówień publicznych dotyczące spełnienia warunków w postępowaniu

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

……
(wpisać nazwę Zadania)

prowadzonego przez Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sejnach, **oświadczam/my, że spełniam/my*** warunki udziału w postępowaniu określone przez Zamawiającego w rozdziale VII SWZ, dotyczące sytuacji ekonomicznej lub finansowej oraz zdolności technicznej lub zawodowej

..... dnia ....
/podpis i pieczątka upoważnionego przedstawiciela/

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 6 do SWZ

Wykonawca

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

Oświadczenie Wykonawcy
składane w zakresie art. 108 ust. 1 pkt. 5 ustawy z dnia 11 września 2019 r.
Prawo zamówień publicznych (Dz.U. poz. 2019 ze zm.) (dalej jako: ustawa Pzp),
dotyczące:
przynależności lub braku przynależności do grupy kapitałowej

Na potrzeby postępowania o udzielenie zamówienia publicznego, pn.:

……
(wpisać nazwę postępowania)

w imieniu:
……
nazwa Wykonawcy
oświadczam/(-my), co następuje:

nie przynależę[1] 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 w niniejszym postępowaniu.

przynależę[1] 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 w niniejszym postępowaniu:

Lp.	Nazwa podmiotu	Adres podmiotu
1		
2		

Uwaga
Wykonawca może przedstawić dokumenty lub informacje potwierdzające przygotowanie oferty niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej.

……. *(miejscowość),* dnia ……..…… r.

……

podpis elektroniczny
osoby/-ób uprawnionej/-ych
do reprezentowania Wykonawcy
lub pełnomocnika

[1] Niepotrzebne skreślić