Samodzielny Publiczny
Zespół Zakładów Opieki Zdrowotnej w Nisku
ul. Kościuszki 1, 37-400 Nisko

Znak sprawy: Z.II.260.036.Zp.2022 Nisko, 29/09/2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

(PO MODYFIKACJI)

zwana dalej (SWZ)

Podnieniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku

Postępowanie o udzielenie zamówienia prowadzone jest na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129 z późn. zm.),, zwanej dalej "ustawą Pzp" w trybie podstawowym bez negocjacji, o wartości szacunkowej zamówienia niższej od progów unijnych określonych na podstawie art. 3 ustawy Pzp.

Zakup finansowany:
- ze środków Funduszu Przeciwdziałania COVID-19

Zatwierdzono w dniu:
29/09/2022

Dyrektor
SPZZOZ w Nisku

Paweł Tofil

/podpisano elektronicznie/

Nisko, Wrzesień 2022

1. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Nisku
ul. Kościuszki 1, 37-400 Nisko
NIP: 865-20-74-945, REGON: 000306680
Tel. (15) 8416 703, 8416 779, Fax. (15) 8416 704
Adres poczty elektronicznej: przetargi@szpital-nisko.pl
Adres strony internetowej: www.szpital-nisko.pl
Adres strony internetowej prowadzonego postępowania oraz strony, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem (adres platformy): https://e-propublico.pl

2. TRYB UDZIELENIA ZAMÓWIENIA

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

3. INFORMACJE OGÓLNE

3.1. Komunikacja w postępowaniu:
W niniejszym postępowaniu komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej, za pośrednictwem platformy on-line działającej pod adresem: https://e-propublico.pl (dalej jako: „Platforma").

3.2. Wizja lokalna:
Zamawiający nie przewiduje obowiązku odbycia przez Wykonawcę wizji lokalnej lub sprawdzenia przez Wykonawcę dokumentów niezbędnych do realizacji zamówienia.

3.3. Zaliczki na poczet wykonania zamówienia:
Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.

3.4. Katalogi elektroniczne:
Zamawiający ☐ wymaga / ☒ nie wymaga złożenia ofert w postaci katalogów elektronicznych.

3.5. Do spraw nieuregulowanych w niniejszej Specyfikacji Warunków Zamówienia mają zastosowanie przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021, poz. 1129 z późn. zm.).

4. OPIS PRZEDMIOTU ZAMÓWIENIA

4.1. Przedmiotem zamówienia jest: Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku.

4.2. Zamawiający dopuszcza składanie ofert częściowych, gdzie część (zadanie) stanowi:

Zadanie nr:	Opis:
1	**Temat:** Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku. **Wspólny Słownik Zamówień:** 32420000-3 - urządzenia sieciowe, 48730000-4 - Pakiety oprogramowania zabezpieczającego. **Opis:** Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku poprzez dostawę, konfigurację i wdrożenie systemu ochrony sieci i komputerów. Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1 do SWZ. **Zamawiający dopuszcza składanie ofert równoważnych, nie dopuszcza składania ofert wariantowych**
2	**Temat:** Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku. **Wspólny Słownik Zamówień:** 48710000-8 - Pakiety oprogramowania do kopii zapasowych i odzyskiwania danych. **Opis:** Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku poprzez: dostawę, konfigurację i wdrożenie Odmiejscowionej Infrastruktury Backupowej (zakup praw do korzystania z usługi Oracle Paas&IaaS Universal Credit). Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1 do SWZ. **Zamawiający dopuszcza składanie ofert równoważnych, nie dopuszcza składania ofert wariantowych**

4.3. Części nie mogą być dzielone przez Wykonawców, oferty nie zawierające pełnego zakresu przedmiotu zamówienia określonego w zadaniu częściowym zostaną odrzucone.

4.4. Wykonawca może złożyć ofertę w odniesieniu do ☒wszystkich części zamówienia ☐ maksymalnej liczby części zamówienia: [ ] ☐tylko jednej części zamówienia.

4.5. Zamawiający dopuszcza składanie ofert równoważnych.
Użyte w opisie przedmiotu zamówienia określenia wskazujące znaki towarowe, nazwy własne, patenty lub pochodzenie przedmiotu zamówienia należy odczytywać wraz z wyrazami „lub równoważne". Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym w opisie przedmiotu zamówienia. Wykonawca, który w ofercie powoła się na stosowanie rozwiązań równoważnych jest obowiązany wykazać, że oferowane przez niego produkty i rozwiązania spełniają wymagania określone przez Zamawiającego.

4.6. Miejsce realizacji: Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Nisku.

5. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 7 I 8 USTAWY PZP.

5.1. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.

6. TERMIN WYKONANIA ZAMÓWIENIA

6.1. Zamówienie musi zostać zrealizowane: w nieprzekraczalnym terminie do dnia 02/11/2022 r.

7. INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU

7.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu oraz spełniają warunki udziału w postępowaniu i wymagania określone w niniejszej SWZ, o których mowa w art. 112 ust. 2 ustawy Pzp:
Zamawiający nie określa warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 ustawy Pzp.

8. PODSTAWY WYKLUCZENIA WYKONAWCY Z POSTĘPOWANIA

8.1. 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. 7 ust. 1 Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022, poz. 835).

8.1.1 Podstawy wykluczenia o których mowa w art. 108 ust. 1 ustawyPzp.
Zamawiający wykluczy Wykonawcę na podstawie art. 108 ust. 1 ustawy Pzp w przypadku wystąpienia którejkolwiek z określonych w nim przesłanek tj.:

8.1.1.1 będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
- udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
- handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
- o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
- finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
- o charakterze terrorystycznym, o którym mowa w art. 115 §20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
- powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769 oraz 2020 r. poz. 2023),
- przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego,

przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,

- o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,
- lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego,

8.1.1.2 jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 8.1.1.1;

8.1.1.3 wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

8.1.1.4 wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

8.1.1.5 jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o do-puszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

8.1.1.6 jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

8.1.2. Podstawy wykluczenia o których mowa w art. 109 ust. 1 ustawy Pzp.
Zamawiający przewiduje wykluczenie Wykonawcy na postawie art. 109 ust. 1 pkt. 4 i 7 ustawy Pzp, tj.:

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

8.1.2.2 który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady.

8.1.3 Z postępowania o udzielenie zamówienia, stosownie do art. 7 ust. 1 pkt. 1-3 Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835), Zamawiający wykluczy Wykonawcę:

- wymienionego w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 765/2006" i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.), zwanego dalej „rozporządzeniem 269/2014" albo wpisanego na listę osób i podmiotów, wobec których są stosowane środki, o których mowa w art. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach

w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. 2022 poz. 835), zwaną dalej „listą" na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt. 3 ww. ustawy;

- 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 Rady 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 ww. ustawy;
- 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 i rozporządzeniu nr 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 ww. ustawy.

8.2. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia, ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

8.3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w 108 ust. 1 pkt. 1, 2 i 5 lub art. 109 ust. 1 pkt. 2-5 i 7-10 ustawy Pzp, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:

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

8.4. Zamawiający oceni, czy podjęte przez Wykonawcę czynności, o których mowa w pkt. 8.3 SWZ są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy. Jeżeli podjęte przez Wykonawcę czynności nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza Wykonawcę.

8.5. W przypadku wspólnego ubiegania się o udzielenie zamówienia żaden z Wykonawców nie może podlegać wykluczeniu z postępowania.

8.6. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania, ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

9. INFORMACJA O WYMAGANYCH DOKUMENTACH ORAZ PRZEDMIOTOWYCH I PODMIOTOWYCH ŚRODKACH DOWODOWYCH

9.1. Wykonawca wraz z ofertą zobowiązany jest złożyć:

Lp.	Wymagany dokument
1.	**Wypełniony formularz ofertowy.**
2.	**Wypełniony formularz cenowy.**
3.	**Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału.** W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepodleganiu wykluczeniu składa każdy z Wykonawców.

Lp.	Wymagany dokument
4.	**Oświadczenie Wykonawcy.** Oświadczenie Wykonawcy, że nie podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 poz. 835).
5.	**Pełnomocnictwo.** W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę nie wymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne pełnomocnictwo w oryginale lub kopii poświadczonej notarialnie.
6.	**Pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia**. (Dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia).
7.	**Zobowiązanie podmiotów trzecich do oddania do dyspozycji niezbędnych zasobów.** Pisemne zobowiązanie podmiotów, na zdolnościach lub sytuacji, których Wykonawca polega, do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia (jeżeli dotyczy).
8.	**Przedmiotowe środki dowodowe.** Dokumenty i materiały informacyjne: specyfikacje techniczne, karty katalogowe, certyfikaty, wpisy, wyniki testów, wydruki ze strony internetowej, oświadczenia Wykonawcy lub Producenta lub dokumenty równoważne opisujące przedmiot zamówienia, potwierdzające zgodność wszystkich wskazanych cech i parametrów urządzeń wymienionych w załączniku nr 1 do specyfikacji warunków zamówienia (OPZ).

9.2. Zamawiający w niniejszym postępowaniu nie żąda złożenia przez Wykonawcę podmiotowych środków dowodowych.

9.3. Na podstawie art. 128 ust. 1 ustawy Pzp, jeżeli Wykonawca nie złoży oświadczenia o którym mowa w art. 125 ust. 1 ustawy Pzp, innych dokumentów lub oświadczeń składanych w postępowaniu lub będą one niekompletne lub będą zawierać błędy, zamawiający wezwie wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie z zastrzeżeniem art. 128 ust. 1 pkt 1) i 2) ustawy Pzp.

10. INFORMACJA DLA WYKONAWCÓW POLEGAJĄCYCH NA ZASOBACH PODMIOTÓW TRZECICH

10.1. 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.

10.2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, zobowiązany jest:

1) 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:
   a) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   b) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   c) 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 roboty budowlane lub usługi, których wskazane zdolności dotyczą.
2) 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.

10.3. Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, a także zbada, czy nie zachodzą wobec tych podmiotów podstawy wykluczenia, które zostały przewidziane względem Wykonawcy w pkt. 8 niniejszej SWZ.

10.4. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzą spełniania przez Wykonawcę warunków udziału w postępowaniu lub zajdą wobec tego

podmiotu podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.

11. INFORMACJE DLA WYKONAWCÓW ZAMIERZAJĄCYCH POWIERZYĆ WYKONANIE CZĘŚCI ZAMÓWIENIA PODWYKONAWCOM

11.1. Wykonawca może powierzyć wykonanie części zamówienia Podwykonawcom.

11.2. Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, podał nazwy, dane kontaktowe oraz przedstawicieli, Podwykonawców zaangażowanych w realizację zamówienia, jeżeli są już znani.

11.3. 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.

12. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

12.1. 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.

12.2. Pełnomocnictwo należy dołączyć do oferty i powinno ono zawierać w szczególności wskazanie:

1) postępowania o udzielenie zamówienie publicznego, którego dotyczy;
2) wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia;
3) ustanowionego pełnomocnika oraz zakresu jego umocowania.

12.3. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, dokument „Oświadczenia o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału", o którym mowa w pkt. 9.1 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.

13. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI

13.1. W niniejszym postępowaniu komunikacja Zamawiającego z Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej, za pośrednictwem Platformy on-line działającej pod adresem: https://e-propublico.pl.

13.2. Korzystanie z Platformy przez Wykonawcę jest bezpłatne.

13.3. Na Platformie postępowanie prowadzone jest pod nazwą: „Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku" – znak sprawy: Z.II.260.036.Zp.2022.

13.4. Wykonawca przystępując do postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z Platformy określone w Regulaminie zamieszczonym na stronie internetowej https://e-propublico.pl oraz uznaje go za wiążący.

13.5. Wykonawca zamierzający wziąć udział w postępowaniu musi posiadać konto na Platformie.

13.6. Do złożenia oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy ważnego kwalifikowanego podpisu elektronicznego, podpisu zaufanego lub podpisu osobistego.

13.7. W sytuacji awarii lub niedostępności Platformy on-line, uniemożliwiających komunikację Wykonawcy i Zamawiającego poprzez Platformę, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres: przetargi@szpital-nisko.pl (nie dotyczy składania ofert).

13.8. 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. 2020 poz. 346);

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. 2020 poz. 332).

13.9. Zalecenia Zamawiającego odnośnie kwalifikowanego podpisu elektronicznego:
a) dokumenty sporządzone i przesyłane w formacie .pdf zaleca się podpisywać kwalifikowanym podpisem elektronicznym w formacie PAdES;
b) dokumenty sporządzone i przesyłane w formacie innym niż .pdf (np.: .doc, .docx, .xlsx, .xml) zaleca się podpisywać kwalifikowanym podpisem elektronicznym w formacie XAdES;
c) do składania kwalifikowanego podpisu elektronicznego zaleca się stosowanie algorytmu SHA-2 (lub wyższego).

13.10. Zamawiający określa następujące wymagania sprzętowo – aplikacyjne pozwalające na korzystanie z Platformy:
a) stały dostęp do sieci Internet,
b) posiadanie dowolnej i aktywnej skrzynki poczty elektronicznej (e-mail),
c) komputer z zainstalowanym systemem operacyjnym Windows 7 (lub nowszym) albo Linux,
d) zainstalowana dowolna przeglądarka internetowa - Platforma współpracuje z najnowszymi, stabilnymi wersjami wszystkich głównych przeglądarek internetowych (Internet Explorer 10+, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera),
e) włączona obsługa JavaScript oraz Cookies.

13.11. Zamawiający dopuszcza następujący format przesyłanych danych:
a) pliki w formatach określonych w załączniku nr 2 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, przy czym zaleca się wykorzystywanie plików w formacie: .pdf, .doc, .docx, .xls, .xlsx,
b) w celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z rozszerzeń: .zip lub .7Z,
c) Maksymalny rozmiar pojedynczego pliku to 80 MB, przy czym nie określa się limitu liczby plików.

13.12. Zamawiający określa następujące informacje na temat kodowania i czasu odbioru danych:
a) załączony i przesłany przez Wykonawcę za pomocą Platformy plik oferty wraz z załącznikami, nie jest dostępny dla Zamawiającego i przechowywany jest na serwerach Platformy w formie zaszyfrowanej. Zamawiający otrzyma dostęp do pliku dopiero po upływie terminu otwarcia ofert,
b) oznaczenie czasu odbioru danych przez Platformę stanowi przyporządkowaną do dokumentu elektronicznego datę oraz dokładny czas (hh:mm:ss), widoczne przy wysłanym dokumencie w kolumnie „Data przesłania”,
c) o terminie przesłania decyduje czas pełnego przeprocesowania transakcji pliku na Platformie.

13.13. W postępowaniu, wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje przekazywane są za pośrednictwem Platformy (karta „Wiadomości”). Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przesłanych za pośrednictwem Platformy, przyjmuje się datę ich zamieszczenia na Platformie.

13.14. Ofertę, wraz ze stanowiącymi jej integralną część załącznikami, składa się pod rygorem nieważności w formie elektronicznej lub postaci elektronicznej za pośrednictwem Platformy, podpisaną kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

13.15. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

13.16. Osobami uprawnionymi do kontaktu z Wykonawcami są:
- w zakresie merytorycznym:
Marek Kurlej – Infortmatyk, tel.: (15) 8416 785, e-mail: m.kurlej@szpital-nisko.pl
Waldemar Daczyński – Infortmatyk, tel.: (15) 8416 785, e-mail: w.daczynski@szpital-nisko.pl
Tomasz Maluga – Zastępca Drektora ds. Ekonomiczno - Administracyjnych, tel.: (15) 8416 701
- w zakresie formalnym:
Piotr Tabor – Specjalista ds. zamówień publicznych, tel.: (15) 8416 779, e-mail: przetargi@szpital-nisko.pl

14. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ TREŚCI SWZ

14.1. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ, przekazanym za pośrednictwem Platformy (karta „Zapytania/Wyjaśnienia").

14.2. 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.

14.3. Jeżeli wniosek o wyjaśnienie treści SWZ nie wpłynie w terminie, o którym mowa w punkcie powyżej, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ.

14.4. Przedłużenie terminu składania ofert, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.

14.5. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępni na stronie internetowej prowadzonego postępowania, bez ujawniania źródła zapytania.

14.6. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej prowadzonego postępowania.

15. WYMAGANIA DOTYCZĄCE WADIUM

15.1. W postępowaniu nie jest przewidziane składanie wadium.

16. TERMIN ZWIĄZANIA OFERTĄ

16.1. Wykonawca pozostaje związany ofertą do dnia **08/11/2022**.

16.2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

16.3. 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.

17. OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

17.1. Wykonawca może złożyć tylko jedną ofertę.

17.2. Treść oferty musi być zgodna z wymaganiami Zamawiającego określonymi w niniejszej SWZ.

17.3. Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy, powinny być sporządzone zgodnie z tymi wzorami.

17.4. Oferta wraz ze stanowiącymi jej integralną część załącznikami musi być sporządzona w języku polskim i złożona pod rygorem nieważności w formie elektronicznej lub postaci elektronicznej, za pośrednictwem Platformy oraz podpisana kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

17.5. Zamawiający informuje, że zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), zwanej dalej „ustawą o zwalczaniu nieuczciwej konkurencji" jeżeli Wykonawca:

a) wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane,

b) wykazał, załączając stosowne uzasadnienie, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

17.6. Zaleca się, aby uzasadnienie o którym mowa powyżej było sformułowane w sposób umożliwiający jego udostępnienie pozostałym uczestnikom postępowania.

17.7. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp.

17.8. Opis sposobu przygotowania oferty składanej w formie elektronicznej lub w postaci elektronicznej:

a) Wykonawca, chcąc przystąpić do udziału w postępowaniu, loguje się na Platformie, w menu **„Ogłoszenia"** wyszukuje niniejsze postępowanie, otwiera je klikając w jego temat, a następnie korzysta z funkcji **„Zgłoś udział w postępowaniu"** na karcie **„Informacje ogólne"**,

b) w przypadku, gdy Wykonawca nie posiada konta na Platformie, należy skorzystać z funkcji **„Zarejestruj"**. Po wypełnieniu Formularza rejestracyjnego Wykonawca otrzyma wiadomość e-mail na

zdefiniowany adres poczty elektronicznej, z opcją aktywacji konta. Aktywacja konta jest konieczna do zakończenia procesu rejestracji i umożliwia zalogowanie się na Platformie,

c) oferta wraz ze stanowiącymi jej integralną część załącznikami, powinna być podpisana ważnym kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę (osoby) uprawnione do reprezentowania Wykonawcy, zgodnie z formą reprezentacji określoną w dokumentach rejestrowych, a następnie przesłana Zamawiającemu za pośrednictwem Platformy, poprzez dodanie dokumentów na karcie **„Oferta/Załączniki”**, za pomocą opcji **„Załącz plik”** i użycie przycisku **„Załącz”**,

d) jeżeli umocowanie dla osób podpisujących ofertę nie wynika z dokumentów rejestrowych, Wykonawca do oferty powinien dołączyć dokument pełnomocnictwa udzielonego przez osoby uprawnione i obejmujące swym zakresem umocowanie do złożenia oferty lub do złożenia oferty i podpisania umowy. Pełnomocnictwo powinno zostać złożone w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym albo w elektronicznej kopii dokumentu poświadczonej notarialnie za zgodność z oryginałem przy użyciu kwalifikowanego podpisu elektronicznicznego,

e) wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji, które Wykonawca chce zastrzec jako tajemnicę przedsiębiorstwa, powinny zostać przesłane za pośrednictwem Platformy, w osobnym pliku, na karcie **„Oferta/Załączniki”**, w tabeli **„Część oferty stanowiąca tajemnicę przedsiębiorstwa”**, za pomocą opcji **„Załącz plik”** i użycie przycisku **„Załącz”**,

f) potwierdzeniem prawidłowo załączonego pliku jest automatyczne wygenerowanie przez Platformę komunikatu systemowego o treści **„Plik został poprawnie przesłany na platformę”**,

g) ostateczne złożenie oferty wraz z załącznikami Wykonawca musi potwierdzić klikając w przycisk **„Złóż ofertę”**,

h) złożenie oferty zostanie potwierdzone komunikatem systemowym z podaniem terminu jej złożenia oraz aktywowana zostanie dla Wykonawcy możliwość pobrania, w stosunku do każdego z przesłanych plików, automatycznie wystawionego przez Platformę dokumentu EPO (Elektroniczne Potwierdzenie Odbioru), będącego dowodem potwierdzającym fakt i czas dostarczenia Zamawiającemu pliku za pośrednictwem Platformy.

17.9. Do upływu terminu składania ofert, Wykonawca, za pośrednictwem Platformy, może wycofać złożoną ofertę, używając opcji **„Wycofaj ofertę”** (karta Oferta/Załączniki). Po wycofaniu oferty Wykonawca może usunąć załączone pliki, zaznaczając pozycje do usunięcia i klikając w przycisk **„Usuń zaznaczone”**.

17.10. Szczegółowa instrukcja korzystania z Platformy znajduje się na stronie internetowej https://e-ProPublico.pl/, przycisk **„Instrukcja Wykonawcy”**.

17.11. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

18. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

18.1. Ofertę, wraz z załącznikami, należy złożyć za pośrednictwem Platformy w terminie do dnia **10/10/2022** do godz. **09:00**.

19. TERMIN OTWARCIA OFERT

19.1. Otwarcie ofert nastąpi w dniu: **10/10/2022** o godz. **09:30**, za pośrednictwem Platformy, na karcie **„Oferta/Załączniki”**, poprzez ich odszyfrowanie, które jest jednoznaczne z ich upublicznieniem.

19.2. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

19.3. Niezwłocznie po otwarciu ofert, Zamawiający zamieści na stronie internetowej prowadzonego postępowania informacje o:

1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej bądź miejscach zamieszkania Wykonawców, których oferty zostały otwarte,
2) cenach lub kosztach zawartych w ofertach.

20. OPIS SPOSOBU OBLICZENIA CENY

20.1. 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.

20.2. 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.

20.3. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich z dokładnością do dwóch miejsc po przecinku.

20.4. Wykonawca zobowiązany jest zastosować stawkę VAT zgodnie z obowiązującymi przepisami ustawy z 11 marca 2004 r. o podatku od towarów i usług.

20.5. 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.

20.6. Wykonawca składając ofertę zobowiązany jest:

1) poinformować Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego,
2) wskazać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego,
3) wskazać wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku,
4) wskazać stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

21. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

21.1. Zamawiający będzie oceniał oferty według następujących kryteriów:

Nr	Nazwa kryterium	Waga
1.	**Cena**	**60 %**
2.	**Warunki płatności**	**40 %**

21.2. Punkty przyznawane za podane kryteria będą liczone według następujących wzorów:

Nr kryterium	Wzór
1.	**Cena (koszt)** **Liczba punktów = (Cmin/Cof) * 100 * waga** **gdzie:** **- Cmin – najniższa cena spośród wszystkich ofert,** **- Cof – cena podana w badanej ofercie**
2.	**Warunki płatności:** **Liczba punktów = (Wof/Wmax) * 100 * waga** **gdzie:** **- Wof – najkrótszy termin płatności podany w badanej ofercie** **- Wmax – najdłuższy termin płatności spośród wszystkich ofert**

Minimalny termin płatności wynosi: 30 dni od dnia doręczenia faktury.

Maksymalny termin płatności wynosi: 60 dni od dnia doręczenia faktury.

Całkowita liczba uzyskanych przez badaną ofertę punktów
= [(Cmin/Cof) * 100 * waga] + [(Wof/Wmax) * 100 * waga]

21.3. Po dokonaniu oceny punkty przyznane przez każdego z członków Komisji przetargowej zostaną zsumowane dla każdego z kryteriów oddzielnie. Suma punktów uzyskanych za wszystkie kryteria oceny stanowić będzie końcową ocenę danej oferty.

21.4. Zamawiający poprawia w ofercie:

a) oczywiste omyłki pisarskie,
b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
c) inne omyłki polegające na niezgodności oferty ze SWZ, niepowodujące istotnych zmian w treści oferty. Zamawiający wyznaczy wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie sposobu jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.

niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

21.5. 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.

21.6. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy.

21.7. 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.

21.8. 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.

22. UDZIELENIE ZAMÓWIENIA

22.1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszej specyfikacji warunków zamówienia i została oceniona jako najkorzystniejsza w oparciu o podane wyżej kryteria oceny ofert.

22.2. 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 https://e-propublico.pl.

22.3. 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.

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

23.1. Zamawiający zawrze umowę w sprawie zamówienia publicznego, w terminie i na zasadach określonych w art. 308 ust. 1 i 2 ustawy Pzp.

23.2. Zamawiający poinformuje Wykonawcę, któremu zostanie udzielone zamówienie, o miejscu i terminie zawarcia umowy.

23.3. Przed zawarciem umowy Wykonawca, na wezwanie Zamawiającego, zobowiązany jest do podania wszelkich informacji niezbędnych do wypełnienia treści umowy.

23.4. 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.

23.5. 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.

24. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

24.1. W danym postępowaniu wniesienie zabezpieczenie należytego wykonania umowy nie jest wymagane.

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

25.1. Wzór umowy stanowi załącznik do niniejszej specyfikacji istotnych warunków zamówienia.

25.2. Zakres dopuszczalności dokonywania zmian postanowień zawartej umowy oraz warunki dokonywania takich zmian określone zostały w projektowanych postanowieniach umowy stanowiących załącznik niniejszej specyfikacji.

26. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

26.1. Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy Pzp, przysługują środki ochrony prawnej na zasadach przewidzianych w art. 505 – 590 ustawy Pzp.

27. AUKCJA ELEKTRONICZNA

27.1. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej, o której mowa w art. 308 ust. 1 ustawy Pzp.

28. OCHRONA DANYCH OSOBOWYCH

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

28.2. Administratorem Państwa danych jest **Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej** 37-400 Nisko, ul. Kościuszki 1, tel.: 15 841 67 03, fax: 15 841 67 04, e-mail: info@szpital-nisko.pl,

28.3. Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu email: adam.zieminski@cbi24.pl lub pisemnie pod adresem Administratora.

28.4. Dane osobowe będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego.

28.5. Dane osobowe będą przetwarzane przez okres zgodnie z art. 78 ust. 1 i 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.), 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.

28.6. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia.

28.7. Odbiorcami Państwa danych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 4 ustawy Pzp.

28.8. Obowiązek podania przez Państwa danych osobowych bezpośrednio Państwa dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z Pzp.

28.9. Osoba, której dane dotyczą ma prawo do:
- dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania,
- w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów Rozporządzenia służy prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa,

28.10. Osobie, której dane dotyczą nie przysługuje:
- w związku z art. 17 ust. 3 lit. b, d lub e Rozporządzenia - prawo do usunięcia danych osobowych,
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 Rozporządzenia,
- na podstawie art. 21 Rozporządzenia - prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c Rozporządzenia.

28.11. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania

dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.

28.12. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 Rozporządzenia, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego lub konkursu ani zmianą postanowień umowy w zakresie niezgodnym z Pzp.

28.13. Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 Rozporządzenia, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.

28.14. W przypadku danych osobowych zamieszczonych przez Administratora w Biuletynie Zamówień Publicznych, prawa, o których mowa w art. 15 i art. 16 Rozporządzenia, są wykonywane w drodze żądania skierowanego do Administratora.

28.15. Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 ust. 1 Rozporządzenia, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, Administrator nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 Rozporządzenia.

28.16. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.

28.17. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 Rozporządzenia, nie może naruszać integralności protokołu oraz jego załączników.

28.18. Ponadto informujemy, że w związku z przetwarzaniem Państwa danych osobowych nie podlegają Państwo decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 Rozporządzenia.

Załącznikami do specyfikacji warunków zamówienia są:

Nr	Nazwa załącznika
1.	**Opis przedmiotu zamówienia**
2.	**Wzór formularza ofertowego**
3.	**Wzór oświadczenia o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału**
4.	**Wzór oświadczenia wykonawcy o nie podlegniu wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 poz. 835)**
5.	**Wzór zobowiązania podmiotów, na których Wykonawca polega, do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia**
6.	**Projektowane postanowienia umowy (dla każdego zadania)**
7.	**Wzór formularza cenowego**

Załącznik nr 1

OPIS PRRZEDMIOTU ZAMÓWIENIA

1. **Ogólna charakterystyka zamówienia:**
   Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku.
2. **W ramach zamówienia Wykonawca wykona następujące zadania obejmujące dostawy i usługi:**
   Zadanie nr 1: Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku poprzez dostawę, konfigurację i wdrożenie systemu ochrony sieci i komputerów,
   Zadanie nr 2: Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku poprzez dostawę, konfigurację i wdrożenie Odmiejscowionej Infrastruktury Backupowej (zakup praw do korzystania z usługi Oracle Paas& IaaS Universal Credit).

Zadanie nr 1

ZESTAWIENIE PARAMETRÓW MINIMALNYCH

SYSTEM OCHRONY SIECI I KOMPUTERÓW				
Lp.	**Element konfiguracji**	**Wymagania minimalne / warunek konieczny**	**Oferowane parametry (podać)**	**Potwierdzenie spełnienia minimalnych wymagań**
1.	**Typ systemu ochrony**	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.		**TAK / NIE**
		Rozwiązanie powinno wspierać następujące tryby pracy: – routing (warstwa 3), – bridge (warstwa 2), – hybrydowy (część jako router, część jako bridge).		**TAK / NIE**
2.	**Wymagania systemowe**	System ochrony powinien spełniać wymagania w niżej wymienionym zakresie: – Obsługa nielimitowanej ilości hostów w sieci chronionej, – Metalowa obudowa o wysokości 1U przeznaczona do montażu w szafie RACK, – Minimalna liczba i typ interfejsów fizycznych: 8 x 1GbE RJ45 (IEEE 1000Base-T), 2 x 1GbE SFP, 2 x 10BgE SFP, – Minimalnie dodatkowe porty: 2x USB 3.0, 1x USB 2.0, 1x Konsola szeregowa (RJ-45 i USB), dedykowany port managmentowy, – Wyświetlacz LCD na przednim panelu z podstawowymi informacjami statusowymi i konfiguracyjnymi, – Minimalna liczba nowych połączeń na sekundę: 180 000, – Minimalna liczba jednoczesnych połączeń: 12 200 000, – Minimalna przepustowość Firewall: 38 Gbps, – Minimalna przepustowość IPS: 9,8 Gbps,		**TAK / NIE**

		– Minimalna przepustowość Threat Protection: 2 Gbps, – Minimalna przepustowość VPN IPsec: 17 Gbps, – Maksymalne opóźnienie pakietów firewall (dla 4 byte UDP): 4 µs, – Minimalna przepustowość SSL/TLS Inspection: 2,4 Gbps, – Minimalna liczba jednoczesnych połączeń SSL/TLS: 55 000, – Ilość użytkowników nielimitowana, – Zintegrowany podwójny dysk SSD do przechowywania oprogramowania, logowania i raportowania o pojemności nie mniejszej niż 240 GB, – możliwość podpięcia dodatkowego, zewnętrznego redundantnego źródła zasilania.		
3.	**Podstawowe funkcje systemu ochrony**	Zarządzanie i utrzymanie: 1. Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. 2. Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 3. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 4. System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności. 5. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.		**TAK / NIE**

		7. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. 8. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. 9. Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej. 10. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP. 11. Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3. 12. System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). 13. System powinien oferować możliwość integracji z centralnym systemem do zarządzania. 14. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego lub via email. 15. Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. 16. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. 17. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud. 18. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). 19. System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu		

		zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive. 20. W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie). 21. Dedykowany układ sprzętowy akcelerujący funkcje filtracji, szyfrowania i deszyfrowania ruchu SSL/TSL.		
4.	**Zapora sieciowa, konfiguracja sieciowa oraz routing**	1. Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas. 3. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 4. Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług. 5. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. 6. System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN. 7. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. 8. Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading. 9. System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 10. System powinien zapewniać ochronę przed skanowaniem portów (portscan blocking). 11. System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 12. Rozwiązanie powinno zapewniać obsługę routingu statycznego. 13. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). 14. System powinien oferować wsparcie dla IGMP snooping. 15. Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy). 16. Rozwiązanie powinno oferować możliwość łączenia interfejsów		**TAK / NIE**

		w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. 17. System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. 18. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. 19. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 20. Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów. 21. Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules. 22. Wymagane jest aby rozwiązanie zapewniało obsługę modemów USB 3G/LTE/UMTS. 23. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 24. System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP. 25. System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania. 26. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).		
5.	**Podstawowe kształtowanie pasma oraz limity ilości danych**	1. System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników. 2. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. 3. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.		**TAK / NIE**
6.	**Bezpieczna sieć bezprzewodowa**	1. System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. 2. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater. 3. Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się		**TAK / NIE**

		na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. 4. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. 5. Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej. 6. Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej. 7. Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. 8. Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication). 9. Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). 10. System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. 11. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. 12. System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden. 13. System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe. 14. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych.		
7.	**Autoryzacja użytkowników**	1. Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication. 2. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. 3. System powinien zapewniać możliwość autentykacji w oparciu o Active		**TAK / NIE**

		Directory, eDirectory, RADIUS, LDAP i TACACS+. 4. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. 5. Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password). 6. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server. 7. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. 8. Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 9. Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.		
8.	**Samoobsługowy portal dla użytkowników**	1. Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci. 2. Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 3. Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows. 4. Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android. 5. Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła. 6. Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika. 7. Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.		**TAK / NIE**
9.	**Podstawowe opcje VPN**	System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: – Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK), – Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny		**TAK / NIE**

		z poziomu samoobsługowego portalu użytkownika).		
10.	**Klient IPSec VPN (dostępny osobno)**	1. Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH. 2. Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512. 3. Wsparcie dla split-tunneling. 4. Wsparcie dla NAT-traversal. 5. Monitorowanie stanu połączenia.		**TAK / NIE**
11.	**Ochrona sieci**	**IPS:** Dodatkowy moduł ochrony klasy IPS z bazą minimum 7100 sygnatur. Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. System powinien generować alerty w przypadku wykrycia ataku.		**TAK / NIE**
		ATP: System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.		**TAK / NIE**
		Synchronizacja z endpoint: System powinien mieć możliwość rozbudowy uruchomienia synchronizacji stanu bezpieczeństwa komputerów w sieci LAN z Firewallem. Możliwość automatycznego odcięcia komputera/ów zainfekowanych. (wymagane dodatkowe oprogramowanie nie będące częścią tego postępowania)		**TAK / NIE**
		Clientless VPN: Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.		**TAK / NIE**
12.	**Ochrona i kontrola Web**	1. Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP). 3. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 4. System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego. Oba silniki powinny pracować równocześnie.		**TAK / NIE**

		5. Rozwiązanie powinno automatyczne odpytywać bazy producenta w trybie rzeczywistym. 6. Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch). 7. Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. Walidacją certyfikatów. 8. System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma. 9. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. 10. Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów, cookies. 11. System powinien zapewniać możliwość emulacji skryptów JavaScript. 12. Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 13. Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 14. Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS. 15. Rozwiązanie powinno umożliwiać blokadę stron HTTPS. 16. Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS. 17. Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do Internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników. 18. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.		
13.	**Ochrona i kontrola aplikacji**	1. Rozwiązanie powinno oferować bazę danych opisująca, co najmniej 3 500 aplikacji. 2. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. 3. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. 4. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania. 5. Rozwiązanie powinno umożliwiać blokowanie:		**TAK / NIE**

		– aplikacji, które pozwalają na transfer plików (np. P2P). – komunikatorów internetowych, przynajmniej Skype, Gadu-gadu. – proxy uruchamianych poprzez przeglądarki internetowe. – streaming media (radio internetowe, Youtube, Vimeo). 6. Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.		
14.	**Kształtowanie pasma dla Web I Aplikacji**	1. Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie. 2. Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym oraz współdzielonym. 4. Rozwiązanie powinno zapewniać możliwość przeglądania kwarantanny z opcją wyszukiwania wiadomości i opcjami filtrowania po dacie, nadawcy, odbiorcy, temacie wraz z opcją zwalniania lub usuwania wiadomości z kwarantanny (przez samoobsługowy portal użytkownika).		**TAK / NIE**
15.	**Ochrona przed exploitami i zagrożeniami zero-day**	**On-cloud Sandboxing:** 1. Rozwiązanie powinno posiadać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox umożliwiający dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll. 2. Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf. 3. Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf. 4. Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym: .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. 5. System zapewniający dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS. 6. System ochrony ze średnim realnym czasem analizy kodu poniżej 120 sekund. 7. System powinien oferować szczegółowe raporty wyników analizy.		**TAK / NIE**

16.	**Logowanie I raportowanie**	1. System powinien umożliwiać składowanie oraz archiwizację logów. 2. System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. 4. System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 5. System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 6. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. 7. Rozwiązanie powinno generować raporty w PDF, HTML i XLS. 8. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych, do co najmniej 3 serwerów syslog. 9. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. 10. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. 11. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. 12. System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora. 13. System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.		**TAK / NIE**
17.	**Pozostałe**	1. Oferowane rozwiązanie powinno być objęte serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. 2. Obsługa gwarancyjna na sprzęt powinna być prowadzona przez producenta		**TAK / NIE**

		w trybie 24 godziny przez 7 dni w tygodniu. 3. Wsparcie techniczne do oprogramowania powinno być prowadzone przez producenta w trybie 24 godziny przez 7 dni w tygodniu. W ramach wsparcia technicznego producent zobowiązany jest do dostarczania aktualizacji i poprawek oprogramowania dla wszystkich dostarczonych modułów.		
18.	**Informacje dodatkowe**	Razem z urządzeniem w postaci hardware appliance należy dostarczyć następujące dodatki: 1. Licencje na okres 60 miesięcy zapewniające pełną podstawową funkcjonalność urządzenia oraz rozbudowę o dodatkowe moduły: zaawansowaną ochronę sieci, ochronę i fitrowanie Web oraz ochronę Sandstorm. 2. Zaawansowane wsparcie producenta na okres równy okresowi licencjonowania zapewniający: – nielimitowany dostęp do poprawek i aktualizacji, – dostęp do nowych funkcji i funkcjonalności w obrębie modułów licencyjnych, – wsparcie telefoniczne i mailowe producenta w trybie 24 x 7, – rozszerzony program napraw gwarancyjnych RMA (wymiana urządzenia na nowe w przypadku awarii). 3. Drugie fizyczne urządzenie umożliwiające budowę klastra w celu zapewnienia funkcjonalności HA systemu i odporności na awarię.		**TAK / NIE**
19.	**Administracja zdalna**	1. Rozwiązanie Centralnej administracji musi wspierać instalację na systemach Windows Server, Linux lub być dostępne jako chmurowa usługa producenta. 2. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 3. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami. 4. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, antyransomware, exploit protection, IPS które działają na stacjach roboczych w sieci.		**TAK / NIE**

		5. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 6. Rozwiązanie musi zapewniać korzystanie z szablonów raportów, przygotowanych przez producenta. 7. Rozwiązanie musi zapewniać podział uprawnień administracyjnych. 8. Maszyny z systemami Windows, Mac i Linux muszą być zarządzane z jednej konsoli zarządzania. 9. Musi mieć możliwość na synchronizację użytkowników/grup/komputerów z lokalnych serwerów Active Directory w celu zarządzania politykami. 10. Tworzone polityki powinny mieć możliwość zastosowania do użytkowników lub urządzeń. 11. Aktualizacja punktów końcowych powinna mieć możliwość ustawienia przepustowości używanej zarówno do aktualizacji oprogramowania, jak i aktualizacji definicji zagrożeń. 12. Rozwiązanie musi mieć możliwość integracji z interfejsem API zgodne z REST.		
20.	**Ochrona stacji roboczych**	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. 3. Rozwiązanie musi klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub niegroźne. 4. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. Rozwiązanie musi zapewniać wykonywanie skanowania zagrożeń Dni Zero (0 day) w trybie offline (bez dostępu do Internetu). 6. Rozwiązanie musi chronić system nawet w trybie offline i nie będzie polegać na sygnaturach. 7. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. 8. Rozwiązanie musi mieć możliwość wywołania czyszczenia stacji po każdym aktywnym wykryciu exploita lub ransomware w oparciu o pliki i procesy.		**TAK / NIE**

		9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. 10. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów minimum HTTPS bez konieczności dystrybuowania certyfikatów. 11. Rozwiązanie musi posiadać wbudowany moduł zapobieganie/ograniczania luk w zabezpieczeniach minimum w oparciu o ochrona wykonywania danych (DEP), randomizację układu przestrzeni adresowej (ASLR), Strukturalna ochrona przed nadpisaniem obsługi wyjątków (SEHOP), DLL Hijacking, Reflective DLL Injection, Stack Pivot, Dynamic Shellcode. 12. Rozwiązanie musi zapewniać ochronę przed atakami przepełnienia bufora. 13. Rozwiązanie musi być w stanie skanować ruch w oparciu o inspekcję pakietów (IPS) na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji. 14. Rozwiązanie musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu sprzed zaszyfrowania i przywróci je do ich pierwotnej lokalizacji. 15. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. 16. Rozwiązanie musi umożliwiać zarówno ochrona Anti-Exploit, jak i Ransomware bez konieczności łączenia z zewnętrzną usługa „Sandboxing” 17. Rozwiązanie musi chronić przed złośliwym kodem (na przykład skryptami PowerShell) za pomocą interfejsu Microsoft Antimalware Scan Interface (AMSI). 18. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów. 19. Rozwiązanie musi być w stanie wykrywać i blokować kategorie aplikacji, które mogą nie być odpowiednie do użytku w środowisku przedsiębiorstw.		

		20. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering. 21. Rozwiązanie musi być w stanie monitorować i konfigurować Zaporę systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory systemu Windows. 22. Rozwiązanie musi mieć opcję generowania migawki kryminalistycznej złośliwej aktywności, która wystąpiła na chronionym punkcie końcowym. 23. Rozwiązanie musi posiadać opcję „automatycznego izolowania" skompromitowanych punktów końcowych od sieci. 24. Rozwiązanie musi mieć możliwość monitorowania lub zatrzymywania lokalnych użytkowników administracyjnych lub złośliwych procesów w celu wyłączenia ochrony punktu końcowego: – Zatrzymywanie usług z interfejsu usług – Zabicia usługi i procesu z interfejsu Menedżera zadań – Zmianę konfigurację usługi w interfejsie usług – Odinstalowania – Usunięcia lub modyfikacji chronionych plików lub folderów – Usunięcia lub modyfikacji chronionych kluczy rejestru 25. Rozwiązanie musi mieć możliwość zidentyfikowania, „co się stało, skąd pochodziło naruszenie, jakie pliki zostały naruszone", oraz dostarczać wskazówek, jak wzmocnić postawę bezpieczeństwa organizacji. 26. Rozwiązanie musi zapewniać widok wszystkiego, co miało wpływ na atak. Pozycje można filtrować według typu. np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdej pozycji m.in. Nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia. 27. Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy.		
21.	**Ochrona Serwerów Windows**	1. Rozwiązanie musi wspierać systemy operacyjne Windows Server2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server2016, Windows Server2019, Windows Server2022.		**TAK / NIE**

		2. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. 3. Rozwiązanie musi klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub niegroźne. 4. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. Rozwiązanie musi zapewniać wykonywanie skanowania zagrożeń Dni Zero (0 day) w trybie offline (bez dostępu do Internetu). 6. Rozwiązanie musi chronić system nawet w trybie offline i nie będzie polegać na sygnaturach. 7. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. 8. Rozwiązanie musi mieć możliwość wywołania czyszczenia stacji po każdym aktywnym wykryciu exploita lub ransomware w oparciu o pliki i procesy 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. 10. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów minimum HTTPS bez konieczności dystrybuowania certyfikatów. 11. Rozwiązanie musi posiadać wbudowany moduł zapobieganie/ograniczania luk w zabezpieczeniach minimum w oparciu o ochrona wykonywania danych (DEP), randomizację układu przestrzeni adresowej (ASLR), Strukturalna ochrona przed nadpisaniem obsługi wyjątków (SEHOP), DLL Hijacking, Reflective DLL Injection, Stack Pivot, Dynamic Shellcode. 12. Rozwiązanie musi zapewniać ochronę przed atakami przepełnienia bufora. 13. Rozwiązanie musi być w stanie skanować ruch w oparciu o inspekcję pakietów (IPS) na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji. 14. Rozwiązanie musi mieć możliwość przywrócenia zaszyfrowanych plików do		

		stanu sprzed zaszyfrowania i przywróci je do ich pierwotnej lokalizacji. 15. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. 16. Rozwiązanie musi umożliwiać zarówno ochrona Anti-Exploit, jak i Ransomware bez konieczności łączenia z zewnętrzną usługa „Sandboxing". 17. Rozwiązanie musi być chronić przed złośliwym kodem (na przykład skryptami PowerShell) za pomocą interfejsu Microsoft Antimalware Scan Interface (AMSI). 18. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów. 19. Rozwiązanie musi być w stanie wykrywać i blokować kategorie aplikacji, które mogą nie być odpowiednie do użytku w środowisku przedsiębiorstw. 20. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering. 21. Rozwiązanie musi być w stanie monitorować i konfigurować Zaporę systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory systemu Windows. 22. Rozwiązanie musi mieć opcję generowania migawki kryminalistycznej złośliwej aktywności, która wystąpiła na chronionym punkcie końcowym. 23. Rozwiązanie musi posiadać opcję „automatycznego izolowania" skompromitowanych punktów końcowych od sieci. 24. Rozwiązanie musi mieć możliwość monitorowania lub zatrzymywania lokalnych użytkowników administracyjnych lub złośliwych procesów w celu wyłączenia ochrony punktu końcowego: – Zatrzymywanie usług z interfejsu usług – Zabicia usługi i procesu z interfejsu Menedżera zadań – Zmianę konfigurację usługi w interfejsie usług – Odinstalowania – Usunięcia lub modyfikacji chronionych plików lub folderów		

		– Usunięcia lub modyfikacji chronionych kluczy rejestru 25. Rozwiązanie musi mieć możliwość zidentyfikowania, „co się stało, skąd pochodziło naruszenie, jakie pliki zostały naruszone”, oraz dostarczać wskazówek, jak wzmocnić postawę bezpieczeństwa organizacji. 26. Rozwiązanie musi zapewniać widok wszystkiego, co miało wpływ na atak. Pozycje można filtrować według typu. np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdej pozycji m.in. Nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia. 27. Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy.		
22.	**Ochrona Serwerów Linux**	1. Rozwiązanie musi wspierać systemy operacyjne w oparciu o architekturę x64, kernel wspierający minimum glibc 2.7 z działająca usługą system z zainstalownaym Bash. 2. Rozwiązanie musi wykrywać wykorzystywanie luk w aplikacjach Linux, w tym uszkodzenia pamięci, nietypowe zachowanie aplikacji i ucieczki z kontenerów. 3. Rozwiązanie musi wykrywać wykorzystywanie luk w podstawowym systemie Linux, takich jak eskalacja uprawnień, manipulowanie mechanizmami bezpieczeństwa (np. SELinux), korzystanie z popularnych metod eksploatacji jądra i ucieczki z kontenerów. 4. Rozwiązanie musi wykrywać utrzymanie dostępu przez ponowne uruchomienie hosta, w tym backdoory jądra lub backdoory w przestrzeni użytkownika 5. Rozwiązanie musi wykrywać zmiany w systemowych plikach binarnych, zmiany konfiguracji, usuwanie plików i tworzenie nietypowych plików. 6. Rozwiązanie musi wykrywać tzw. ruch boczny, zachowanie usług sieciowych i podsłuchiwanie sieci. 7. Rozwiązanie musi wykrywać nieprawidłowe wykonanie procesu, użycie kompilatora, debugowanie, zaplanowane zmiany zadań. 8. Rozwiązanie musi wykrywać uprzywilejowane użycie poleceń, ryzykowne działania programistów i zmiany kont użytkowników.		**TAK / NIE**

23.	**Endpoint Detection and Response**	1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows, MacOS, Linux współpracujący z systemem do ochrony stacji roboczych i serwerów tego samego producenta. 2. Rozwiązanie musi mieć możliwość późniejszego rozszerzenia moduły EDR o logi pochodzące z platform Android, iOS tego samego producenta. 3. Rozwiązanie musi pozwolić administratorom odszukać informację dotyczące incydentów związanych z bezpieczeństwem, zapewniając wgląd w zakres ataku, sposób jego rozpoczęcia, wpływ i sposób reagowania. 4. Rozwiązanie musi mieć możliwość uruchamiania zapytań zabezpieczających na wszystkich zarządzanych urządzeniach, nawet jeśli są one offline. 5. Rozwiązanie musi mieć opcję „ręcznego izolowania" chronionych punktów końcowych od sieci podczas badania przypadku zagrożenia. 6. Rozwiązanie musi zapewnić interfejs wiersza poleceń umożliwiający zdalny dostęp do urządzeń w celu przeprowadzenia dalszego dochodzenia lub podjęcia odpowiednich działań. Opcja dostępu zdalnego musi być dostępna tylko dla kont administratorów korzystających z uwierzytelniania wieloskładnikowego (MFA). 7. Zdalny dostęp musi być realizowany dla systemów operacyjnych takich jak Windows, Mac i Linux a aktywności zapisane w logach audytowych. 8. Rozwiązanie musi umożliwiać wyszukiwanie szczegółów dotyczących wykonanych poleceń w PowerShell. 9. Rozwiązanie musi zapewniać detekcję w oparciu o Mitre ATT&CK Tactic and Technique. 10. Rozwiązanie musi pozwalać na wysyłanie powiadomień do administratora w chwili utworzenia nowego dochodzenia.		**TAK / NIE**
24.	**Informacje dodatkowe**	Razem należy dostarczyć: 1. 3 szt. punktów dostępowych kompatybilnych z dostarczonymi firewall'ami o minimalnej przepustowości 867 Mbps (5 GHz) + 867 Mbps (5 GHz) zarządzanego z poziomu oferowanego Firewalla. Minimalnie 1x RJ45 10/100/1000 Ethernet w/PoE (802.3af). Możliwość zamontowania na ścianie. Do punktów dostępowych należy dostarczyć dedykowane zasilacze PoE. 2. 200 licencji na końcówki klienckie. 3. 50 licencji na serwery.		**TAK / NIE**

		4. Licencje na okres 60 miesięcy (końcówki/serwery). 5. Zaawansowane wsparcie producenta na okres równy okresowi licencjonowania zapewniający: – nielimitowany dostęp do poprawek i aktualizacji, – dostęp do nowych funkcji i funkcjonalności w obrębie modułów licencyjnych, – wsparcie telefoniczne i mailowe producenta w trybie 24 x 7. 6. Urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału dystrybucyjnego w UE - wymagane oświadczenie wykonawcy lub producenta - i zostały wyprodukowane nie dawniej niż 3 miesiące przed ich dostarczeniem. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia urządzenia w postaci oświadczenia producenta. Zamawiający żąda, aby urządzenia były fabrycznie nowe tj. fabrycznie zapakowane, nieużywane w innych projektach ani testach. Nie dopuszcza się produktów refabrykowanych i odnawianych.		
25.	**Uwagi dodatkowe**	Dostarczone rozwiązanie sprzętowe oraz programowe musi być kompatybilne z już istniejącym rozwiązaniem jakie posiada Zamawiający to jest: Sophos XG310. W przypadku dostawy innego rozwiązania wymagana będzie dostawa dodatkowych urządzeń i licencji kompatybilnych z w/w produktem oraz infrastrukturą Zamawiającego w celu zastąpienia obecnego stosowanego rozwiązania. Dodatkowo wymagane będzie przeprowadzenie testów kompatybilności oraz dodatkowych szkoleń w wymiarze minimum 48 godzin.		**TAK / NIE**
		Wykonawca rozwiązania równoważnego przejmuje na siebie odpowiedzialność za pełne funkcjonowanie dostarczonego rozwiązania na infrastrukturze Zamawiającego.		**TAK / NIE**
		Wykonawca dostarczy Voucher na szkolenie w zakresie konfiguracji dostarczonych urządzeń min. 3 dniowe dla 2 administratorów Zamawiającego prowadzone w certyfikowanym ośrodku szkoleniowym prowadzone przez certyfikowanego instruktora, dopuszczalny jest distance learning. Szkolenie prowadzane w języku polskim. Zapewnienie materiałów edukacyjnych.		**TAK / NIE**

Zadanie nr 2

ZESTAWIENIE PARAMETRÓW MINIMALNYCH

ODMIEJSCOWIONA INFRASTRUKTURA BACKUPOWA (prawo do korzystania z usługi Oracle Paas&IaaS Universal Credit)				
1.	**Usługa backupu**	Usługa backupu świadczona będzie zgodnie z warunkami i zasadami zawartymi w dokumencie *„Oracle PaaS and IaaS Universal Credits Service Descriptions”*, publikowanymi przez dostawcę usługi chmurowej na stronie: http://www.oracle.com/us/corporate/contracts/paas-iaas-universal-credits-3940775.pdf		**TAK / NIE**
		Usługa świadczona będzie nie krócej niż przez 12 kolejnych miesięcy od dnia podpisania Umowy, poprzez udostępnienie na potrzeby Zamawiającego Universal Credits w ilości umożliwiającej tworzenie backupu bazy danych Oracle z wykorzystaniem co najmniej narzędzia RMAN o pojemności nie mniejszej niż 2 TB		**TAK/NIE**
2.	**Wymagania**	Zamawiający wymaga aby Wykonawca był partnerem Oracle, posiadającym prawo odsprzedaży usług chmurowych dla Sektora Publicznego w Polsce, który podpisał z Oracle Polska Sp. z o.o. dodatek dotyczący sektora publicznego do Ramowej Umowy Dystrybucyjnej w ramach Programu Oracle Partner Network oraz załącznik dotyczący sektora publicznego do dodatku dotyczącego dystrybucji usług w chmurze do Ramowej Umowy Dystrybucyjnej w ramach Programu Oracle Partner Network		**TAK/NIE**
		Wykonawca zobowiązany jest dostarczyć Zamawiającemu potwierdzenie nabycia praw do korzystania z usługi do dnia zawarcia umowy.		**TAK/NIE**
3.	**Usługa równoważna usłudze Oracle Paas& IaaS Universal Credit**	Za usługę równoważną Zamawiający uzna taką, która spełniać będzie poniższe warunki: 1) umożliwia dostęp do usług chmurowych typu Platform as a Services (PaaS) oraz Infrastructure as a Service (IaaS) bez określania, jakie to mają być usługi i bez konieczności oddzielnego zakupu licencji (niezbędne do uruchomienia i funkcjonowania usługi licencje będą dostępne w modelu „License Included”), 2) Zamawiający będzie mógł dowolnie zmieniać usługi, z jakich będzie korzystał w okresie realizacji zamówienia, 3) zakres zastosowania technologii zapewni Zamawiającemu możliwość implementacji funkcjonalności, które Zamawiający realizuje w oparciu o technologię Oracle, w szczególności umożliwi Zamawiającemu tworzenie backupu bazy danych systemu		**TAK/NIE**

		szpitalnego AMMS produkcji Asseco SA (Asseco Medical Management System) opartego o bazę danych Oracle w wersji Standard nie niższej niż 11.2, bez konieczności zakupu dodatkowych licencji, wykonywania dodatkowych prac dostosowawczych czy migracji, 4) będzie współdziałać z pozostałymi systemami Zamawiającego zbudowanymi w oparciu o technologię Oracle, wdrożonymi u Zamawiającego, do których Zamawiający posiada prawa licencyjne oraz będzie zapewniać pracę tych systemów tak jak realizuje to technologia Oracle, bez konieczności zakupu dodatkowych licencji, wykonywania dodatkowych prac dostosowawczych czy migracji, 5) nie będzie powodować zakłóceń pracy oprogramowania z zakresu technologii Oracle, z którym będzie współdziałało, 6) zapewni pełną, równoległą pracę w czasie rzeczywistym oraz pełną funkcjonalną zamienność technologii równoważnej z technologią Oracle, 7) umożliwi wskazanie miejsca przetwarzania danych na terenie Europejskiego Obszaru Gospodarczej (EOG, ang. European Economic Area) i uniemożliwi ich przekazanie przez procesora w jakiejkolwiek formie (np. backup, logi) poza ten obszar.		
4.	**Zakres prac**	Zakres prac obejmuje: ~~1) Dostarczenie licencji i dokumentów potwierdzających nabycie praw do licencji,~~ 2) Konfigurację środowiska produkcyjnego, 3) Zaimportowanie bazy danych z kopii bazy Zamawiającego, 4) Uruchomienie usług, ~~5) Testy adaptacyjne minimum 48 roboczogodzin,~~ 6) Przeszkolenie 2 administratorów Zamawiającego w zakresie wdrożonego rozwiązania minimum 8 roboczogodzin, 7) Wsparcie i aktualizacja usług minimum 48 roboczogodzin przez okres świadczenia usług.		**TAK / NIE**

Załącznik nr 2

WZÓR FORMULARZA OFERTY

Wykonawca:

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

reprezentowany przez:

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Zamawiający:

Samodzielny Publiczny
Zespół Zakładów Opieki Zdrowotnej w Nisku
ul. Kościuszki 1
37-400 Nisko

Odpowiadając na ogłoszenie o postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji znak Z.II.260.036.Zp.2022 ogłoszonym zgodnie z przepisami ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129 z późn. zm.) w Biuletynie Zamówień Publicznych w dniu ___/___/2022, pozycja _____ oraz na oraz na Platformie działającej pod adresem https://e-propublico.pl/ na: **„Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku."** oferujemy realizację dostaw i usług objętych zamówieniem, zgodnie z wymogami Opisu Przedmiotu Zamówienia za cenę: _____ zł (bez VAT), słownie: _____

Cena brutto (z VAT) _____ zł, słownie: _____

ZADANIE NR 1	Cena netto (bez VAT):	zł	słownie:
	Cena brutto (z VAT):	zł	słownie:
ZADANIE NR 2	Cena netto (bez VAT):	zł	słownie:
	Cena brutto (z VAT):	zł	słownie:

Termin płatności oferowany zamawiającemu za realizację przedmiotu zamówienia wynosi do 60 dni, tj. _____ dni od daty dostarczenia faktury.

1. Oświadczam, że zapoznaliśmy się ze specyfikacją warunków zamówienia i nie wnosimy do niej zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty.
2. Oświadczam, że uważamy się za związanych niniejszą ofertą przez czas wskazany w specyfikacji warunków zamówienia tj. do dnia: _____.
3. Dostawy objęte zamówieniem zamierzamy wykonać sami / zamierzamy zlecić podwykonawcom.
4. Oświadczam, że zawarte w specyfikacji warunków zamówienia projektowane postanowienia umowy zostały przez nas zaakceptowane i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na wyżej wymienionych warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.
5. Osoba(y) uprawnione do podpisania umowy: _____
6. Adres do korespondencji e-mail: _____
7. Oświadczam, że jesteśmy mikro/małym/średnim/dużym przedsiębiorstwem.*
8. Na podst. art. 225 Ustawy Pzp oświadczam, że wybór oferty będzie/nie będzie* prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.

9. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art.14 RODO (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)) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**
10. Załącznikami do niniejszej oferty są:
    (1) _____
    (2) _____
    (3) _____
    (4) _____
    (5) _____
    (6) _____

* - Niepotrzebne skreślić
** - 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)

Miejscowość ..... dnia

podpis osoby uprawnionej do składania oświadczeń woli
w imieniu Wykonawcy

Załącznik nr 3

Wykonawca:

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

reprezentowany przez:

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Zamawiający:

Samodzielny Publiczny
Zespół Zakładów Opieki Zdrowotnej w Nisku
ul. Kościuszki 1
37-400 Nisko

O Ś W I A D C Z E N I E W Y K O N A W C Y

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

Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129 z późn. zm.) (dalej jako: ustawa Pzp) dotyczące:

PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA
ORAZ SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego prowadzonego w **trybie podstawowym bez negocjacji** na: **Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku**
Oświadczam, co następuje:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Ustawy Pzp.
2. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. _____ ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 lub spośród wymienionych w art. 109 ust. 1 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:

_____

Miejscowość ..... dnia ....
podpis osoby uprawnionej do składania oświadczeń woli
w imieniu Wykonawcy

OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Oświadczam, że spełniam, określone przez Zamawiającego warunki udziału w postepowaniu:

Lp.	Warunki udziału w postępowaniu

Miejscowość ..... dnia ....
podpis osoby uprawnionej do składania oświadczeń woli
w imieniu Wykonawcy

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI

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

Miejscowość ..... dnia ....
podpis osoby uprawnionej do składania oświadczeń woli
w imieniu Wykonawcy

Załącznik nr 4

Wykonawca:

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

reprezentowany przez:

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Zamawiający:

Samodzielny Publiczny
Zespół Zakładów Opieki Zdrowotnej w Nisku
ul. Kościuszki 1
37-400 Nisko

OŚWIADCZENIE WYKONAWCY

O niepodleganiu wykluczeniu 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.

Na potrzeby postępowania o udzielenie zamówienia publicznego, pn.: „**Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku"**

oświadczam, że:

a) nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 poz. 835), zgodnie z którym z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych wyklucza się:
   1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
   2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
   3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3.

Zobowiązuję się do niezwłocznego poinformowania Zamawiającego o zmianie tego stanu.

Jeśli zachodzą podstawy wykluczenia to Wykonawca składa oświadczenie o następującej treści:

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia, o których mowa w art. 7 ust. 1 pkt. …….. ustawy/*wskazać właściwy punkt z powyższych*/.

Zobowiązuję się do niezwłocznego poinformowania Zamawiającego o zmianie tego stanu.

Miejscowość ..... dnia .....

.....
podpis osoby uprawnionej do składania oświadczeń woli
w imieniu Wykonawcy

Załącznik nr 5

ZOBOWIĄZANIE PODMIOTU TRZECIEGO
do oddania do dyspozycji Wykonawcy niezbędnych zasobów
na okres korzystania z nich przy wykonaniu zamówienia

Oświadczam w imieniu _____
/nazwa Podmiotu na zasobach, którego Wykonawca polega/

że oddaję do dyspozycji Wykonawcy _____
/nazwa i adres Wykonawcy/

niezbędne zasoby _____
/zakres zasobów, które zostaną udostępnione Wykonawcy, np. kwalifikacje zawodowe, doświadczenie, potencjał techniczny/

na okres korzystania z nich przy wykonywaniu zamówienia pn.: **Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku** prowadzonego przez Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Nisku

Oświadczam, że:

1. Udostępniam Wykonawcy w/w zasoby w następującym zakresie:
   _____
2. Sposób wykorzystania udostępnionych przeze mnie zasobów przy wykonywaniu zamówienia publicznego będzie następujący:
   _____
3. Zakres i okres mojego udziału przy wykonywaniu zamówienia będzie następujący:
   _____

Miejscowość ..... dnia .....

.....
podpis osoby uprawnionej do składania oświadczeń woli
w imieniu podmiotu na zasobach którego Wykonawca polega

Załącznik nr 6

PROJEKTOWANE POSTANOWIENIA UMOWY

U M O W A
Nr ___/Zp/2022
Zawarta zgodnie z przepisami ustawy Prawo zamówień publicznych

W dniu ___/___/2022 r. pomiędzy **Samodzielnym Publicznym Zespołem Zakładów Opieki Zdrowotnej w Nisku** z siedzibą przy ul. Kościuszki 1, 37-400 Nisko, reprezentowanym przez:
1. _____

Zarejestrowanym w Sądzie Rejonowym w Rzeszowie, XII Wydział Gospodarczy KRS, pod numerem: 0000028548, NIP: 865-20-74-945, REGON 000306680, zwanym dalej „Zamawiającym" a:

_____

reprezentowanym przez:
1. _____

Zarejestrowanym w Sądzie Rejonowym w _____, ____ Wydział Gospodarczy KRS, pod numerem _____ NIP: _____, posiadającym kapitał zakładowy: _____ zł. wpłacony w całości, zwanym dalej „Wykonawcą"

Zgodnie z wynikami postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym bez negocjacji na podstawie art. 275 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (zwanej dalej także: Ustawą Pzp), nr Z.II.260.036.Zp.2022 z dnia 29/09/2022 r. o wartości szacunkowej niższej niż progi unijne, określone na podstawie art. 3 ustawy Pzp zawarta zostaje umowa o treści następującej:

§1.
PRZEDMIOT UMOWY

1. Przedmiotem umowy jest **podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku** poprzez realizację zadania polegającego na dostawie, konfiguracji i wrożeniu systemu ochrony sieci i komputerów zgodnie ze złożoną ofertą z dnia ___/___/2022 r. stanowiącą załącznik nr 2 do niniejszej umowy.
2. Szczegółowy opis przedmiotu zamówienia określony został w załączniku nr 1 do specyfikacji istotnych warunków zamówienia, stanowiącym załącznik nr 1 i integralną część niniejszej umowy.

§2.
TERMIN REALIZACJI

1. Wykonawca wykona Przedmiot Umowy określony w §1 w terminie nieprzekraczalnym terminie do dnia 2 listopada 2022 r.

§3.
WARUNKI PŁATNOŚCI

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 wystawienia faktury. Jeżeli Zamawiający otrzyma fakturę po upływie 5 dni od daty jej wystawienia, termin płatności liczy się od dnia doręczenia faktury Zamawiającemu.
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: info@szpital-nisko.

§4.
ZESPÓŁ

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 trakcie obowiązywania Umowy Wykonawcy przysługiwać będzie prawo do zastępowania za zgodą Zamawiającego członków personelu Wykonawcy innymi osobami, o co najmniej takich samych odpowiednio kwalifikacjach lub doświadczeniu. Zamawiający dokona akceptacji zmiany osób wskazanych do realizacji Umowy w ciągu 3 dni od zgłoszenia jej przez Wykonawcę.
4. W przypadku zmiany osoby wskazanej na danym stanowisku, danej roli, osoba zastępująca musi posiadać odpowiednio doświadczenie zawodowe i/lub kwalifikacje nie gorsze niż osoba zastępowana.
5. Zasady opisane w ust. 3 i 4 będą miały zastosowanie również w przypadku wskazania przez Wykonawcę dodatkowych osób do skierowanych do realizacji przedmiotu umowy.
6. Zamawiający ma prawo zażądać zmiany członka personelu Wykonawcy w przypadku pojawienia się uzasadnionych zastrzeżeń, co do jego kwalifikacji, wiedzy, rzetelności lub terminowości wykonywania obowiązków. Zamawiający zobowiązany jest przekazać zastrzeżenia w formie pisemnej. W takim przypadku Wykonawca dokona zmiany członka personelu na nowego, nie później niż w terminie 5 dni od zgłoszenia zastrzeżeń przez Zamawiającego. Wykonawca zobowiązany jest poinformować Zamawiającego o zaprzestaniu wykonywania prac przez danego członka personelu Wykonawcy, w terminie 7 dni od nastąpienia tego zdarzenia. Każda zmiana personelu, o której mowa powyżej, skutkuje odbiorem lub nadaniem uprawnień do systemów przez Zamawiającego.
7. Zmiana osób, o której mowa powyżej, nie stanowi zmiany Umowy i nie wymaga zawarcia aneksu do Umowy. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o powyższej zmianie w formie pisemnej oraz zapewnienia transferu wiedzy pomiędzy osobami zastępowaną i zastępującą, jak również realizacji innych obowiązków wynikających z Umowy względem nowego członka personelu.
8. 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.
REALIZACJA UMOWY

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 wymaganą od czołowych przedsiębiorstw IT w Polsce 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 powierzenia przetwarzania danych osobowych, na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119.1), której wzór stanowi Załącznik nr 4 do Umowy.

§6.
ODBIÓR PRAC

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.
KARY UMOWNE

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

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   - 5% wartości niezrealizowanej części zamówienia netto gdy Zamawiający odstąpi od umowy z powodu okoliczności, za które odpowiada Wykonawca.
   - 0,2% 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. Strony zastrzegają możliwość dochodzenia odszkodowania przenoszącego wartość kar umownych.

§8.
ODSTĄPIENIE OD UMOWY I WYPOWIEDZENIE

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 takim wypadku Zamawiający wyznaczy Wykonawcy dodatkowy 5-dniowy termin na wykonanie zobowiązania. Jeśli Wykonawca nie rozpocznie w ww. terminie wykonywania przedmiotu umowy w sposób należyty, Zamawiający ma prawo wypowiedzieć umowę ze skutkiem na dzień złożenia wypowiedzenia,
   2) naruszył bezpieczeństwo informacji lub zasady z nim związane.
3. W przypadku zwłoki w realizacji przedmiotu Umowy przekraczającej 7 dni ponad termin wskazany w §2 ust. 1 Zamawiający może, niezależnie od nałożenia na Wykonawcę kar umownych, odstąpić od umowy w całości lub

w części. Termin ten ulega odpowiedniemu przesunięciu o czas trwania opóźnień, które wynikły z winy Zamawiającego.

4. Oświadczenie o odstąpieniu lub wypowiedzeniu powinno być złożone na piśmie i zostać dostarczone drugiej Stronie.
5. Zamawiający może odstąpić od Umowy w terminie 30 dni od daty zaistnienia zdarzenia stanowiącego podstawę do odstąpienia.
6. Odstąpienie od umowy nie wpływa na obowiązek zachowania poufności informacji.
7. W razie odstąpienia od umowy lub jej wypowiedzenia, Zamawiający – w ramach należnego Wykonawcy wynagrodzenia - nabywa autorskie prawa majątkowe i zależne prawa autorskich do utworów oraz utworów i ich nośników, odnośnie do których Zamawiający praw nie nabył, w zakresie określonym w §9, z chwilą złożenia oświadczenia o odstąpieniu lub wypowiedzeniu.
8. 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 (3) tygodni, Strony spotkają się i w dobrej wierze rozpatrzą celowość i warunki rozwiązania umowy.

§9.
PRAWA AUTORSKIE

1. Wykonawca oświadcza, że będą mu przysługiwały autorskie prawa majątkowe i prawa zależne do wszelkich utworów, które powstaną w wyniku wykonania Umowy.
2. Wykonawca, z dniem podpisania protokołu odbioru Raportu, przenosi na Zamawiającego autorskie prawa majątkowe do Raportu, na następujących polach eksploatacji:
   1) w zakresie utrwalania i zwielokrotniania Raportu, - wytwarzanie określoną techniką egzemplarzy, w tym drukarską reprograficzną, elektroniczną, fotograficzną, cyfrową, audiowizualną, technikami multimedialnymi oraz zapisu magnetycznego obejmujące trwałe lub czasowe utrwalanie lub zwielokrotnianie w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu bez ograniczeń co do ilości egzemplarzy oraz korzystania i rozporządzania tymi egzemplarzami;
   2) w zakresie obrotu oryginałem albo egzemplarzami, na których Raportu utrwalono - wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
   3) w zakresie rozpowszechniania Raportu, w sposób inny niż określony w pkt 2 - publiczne wykonanie, wyświetlenie, odtworzenie, nadanie i reemitowanie, a także publiczne udostępnienie Raportu, w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym.
3. Wykonawca przenosi na rzecz Zamawiającego, z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, prawo zezwalania na wykonanie zależnego prawa autorskiego, w tym do rozporządzania i korzystania z opracowań Raportu, w nieograniczonym zakresie, w szczególności w zakresie pól eksploatacyjnych wskazanych w ust. 2.
4. Z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, Zamawiający nabywa na własność egzemplarze Raportu, przekazane przez Wykonawcę oraz nośniki, na których Raport utrwalono.
5. Zamawiający nie ponosi odpowiedzialności za naruszenie autorskich praw majątkowych lub osobistych wobec osób trzecich. Wykonawca zobowiązuje się do nieodwołalnego i bezwarunkowego zwolnienia Zamawiającego,

na pierwsze żądanie, z wszelkich roszczeń, wynikających z naruszenia majątkowych i osobistych praw autorskich, do którego doszło z przyczyn leżących po stronie Wykonawcy.

6. Wykonawca oświadcza, że przygotowany przez niego Raport będzie oryginalny i nie będzie naruszał praw osób trzecich oraz będzie wolny od wad. Wykonawca zobowiązuje się, że w momencie przekazywania Raportu Zamawiającemu będzie wyłącznym ich dysponentem majątkowym praw autorskich.
7. Przeniesienie autorskich praw majątkowych zostaje dokonane na czas nieokreślony i jest nieograniczone terytorialnie.
8. W przypadku ujawnienia nowego pola eksploatacji mającego znaczenie dla Zamawiającego, Strony ustalają, że Wykonawca na wezwanie Zamawiającego przeniesie na Zamawiającego, w terminie 14 dni od doręczenia Wykonawcy wezwania, autorskie prawa majątkowego do Raportu oraz prawo zezwalania na wykonywanie praw zależnych do Raportu na nowym polu eksploatacji, na zasadach określonych w niniejszej umowie. Przeniesienie praw, o których mowa w zdaniu poprzednim, zostanie dokonane na rzecz Zamawiającego w ramach wynagrodzenia przewidzianego niniejszą umową.

§10.
ROZSTRZYGANIE SPORÓW

1. 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.
OCHRONA INFORMACJI

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, którego wzór stanowi Załącznik nr 3 do Umowy. 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.
ZMIANY DO UMOWY

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.
POSTANOWIENIA KOŃCOWE

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.

WYKONAWCA: **ZAMAWIAJĄCY:**

Spis załączników:
Załącznik nr 1 – Opis przedmiotu zamówienia,
Załącznik nr 2 – Oferta Wykonawcy.

U M O W A
Nr ___/Zp/2022
Zawarta zgodnie z przepisami ustawy Prawo zamówień publicznych

W dniu ___/___/2022 r. pomiędzy **Samodzielnym Publicznym Zespołem Zakładów Opieki Zdrowotnej w Nisku** z siedzibą przy ul. Kościuszki 1, 37-400 Nisko, reprezentowanym przez:
1. _____

Zarejestrowanym w Sądzie Rejonowym w Rzeszowie, XII Wydział Gospodarczy KRS, pod numerem: 0000028548, NIP: 865-20-74-945, REGON 000306680, zwanym dalej „Zamawiającym" a:

_____

reprezentowanym przez:
1. _____

Zarejestrowanym w Sądzie Rejonowym w _____, ____ Wydział Gospodarczy KRS, pod numerem _____ NIP: _____, posiadającym kapitał zakładowy: _____ zł. wpłacony w całości, zwanym dalej „Wykonawcą"

Zgodnie z wynikami postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym bez negocjacji na podstawie art. 275 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (zwanej dalej także: Ustawą Pzp), nr Z.II.260.036.Zp.2022 z dnia 29/09/2022 r. o wartości szacunkowej niższej niż progi unijne, określone na podstawie art. 3 ustawy Pzp zawarta zostaje umowa o treści następującej:

§1.
PRZEDMIOT UMOWY

1. Przedmiotem umowy jest **podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Nisku** poprzez realizację zadania polegającego na dostawie, konfiguracji i uruchomieniu Odmiejscowionej Infrastruktury Backupowej (zakup praw do korzystania z usługi Oracle Paas&IaaS Universal Credit) zgodnie ze złożoną ofertą z dnia __/__/2022 r. stanowiącą załącznik nr 2 do niniejszej umowy.
2. Szczegółowy opis przedmiotu zamówienia określony został w załączniku nr 1 do specyfikacji istotnych warunków zamówienia, stanowiącym załącznik nr 1 i integralną część niniejszej umowy.

§2.
TERMIN REALIZACJI

1. Wykonawca wykona Przedmiot Umowy określony w §1 w terminie nieprzekraczalnym terminie do dnia 2 listopada 2022 r.

§3.
WARUNKI PŁATNOŚCI

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 wystawienia faktury. Jeżeli Zamawiający otrzyma fakturę po upływie 5 dni od daty jej wystawienia, termin płatności liczy się od dnia doręczenia faktury Zamawiającemu.
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: info@szpital-nisko.

§4.
ZESPÓŁ

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 trakcie obowiązywania Umowy Wykonawcy przysługiwać będzie prawo do zastępowania za zgodą Zamawiającego członków personelu Wykonawcy innymi osobami, o co najmniej takich samych odpowiednio kwalifikacjach lub doświadczeniu. Zamawiający dokona akceptacji zmiany osób wskazanych do realizacji Umowy w ciągu 3 dni od zgłoszenia jej przez Wykonawcę.
4. W przypadku zmiany osoby wskazanej na danym stanowisku, danej roli, osoba zastępująca musi posiadać odpowiednio doświadczenie zawodowe i/lub kwalifikacje nie gorsze niż osoba zastępowana.
5. Zasady opisane w ust. 3 i 4 będą miały zastosowanie również w przypadku wskazania przez Wykonawcę dodatkowych osób do skierowanych do realizacji przedmiotu umowy.
6. Zamawiający ma prawo zażądać zmiany członka personelu Wykonawcy w przypadku pojawienia się uzasadnionych zastrzeżeń, co do jego kwalifikacji, wiedzy, rzetelności lub terminowości wykonywania obowiązków. Zamawiający zobowiązany jest przekazać zastrzeżenia w formie pisemnej. W takim przypadku Wykonawca dokona zmiany członka personelu na nowego, nie później niż w terminie 5 dni od zgłoszenia zastrzeżeń przez Zamawiającego. Wykonawca zobowiązany jest poinformować Zamawiającego o zaprzestaniu wykonywania prac przez danego członka personelu Wykonawcy, w terminie 7 dni od nastąpienia tego zdarzenia. Każda zmiana personelu, o której mowa powyżej, skutkuje odbiorem lub nadaniem uprawnień do systemów przez Zamawiającego.
7. Zmiana osób, o której mowa powyżej, nie stanowi zmiany Umowy i nie wymaga zawarcia aneksu do Umowy. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o powyższej zmianie w formie pisemnej oraz zapewnienia transferu wiedzy pomiędzy osobami zastępowaną i zastępującą, jak również realizacji innych obowiązków wynikających z Umowy względem nowego członka personelu.
8. Osobami uprawnionymi do bieżących kontaktów w ramach realizacji przedmiotu umowy oraz do odbioru Raportu i podpisywania protokołów są osoby:
   3) po stronie Zamawiającego: Pan/i _____ e-mail: _____
   4) po stronie Wykonawcy: Pan/i _____ e-mail: _____

§5.
REALIZACJA UMOWY

1. Zamawiający zobowiązuje się do współdziałania z Wykonawcą, w szczególności poprzez:
   3) współpracę w zakresie planowania przez Wykonawcę czynności w zakresie realizacji przedmiotu Umowy,
   4) 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 wymaganą od czołowych przedsiębiorstw IT w Polsce 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 powierzenia przetwarzania danych osobowych, na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119.1), której wzór stanowi Załącznik nr 4 do Umowy.

§6.
ODBIÓR PRAC

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.
KARY UMOWNE

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

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   - 5% wartości niezrealizowanej części zamówienia netto gdy Zamawiający odstąpi od umowy z powodu okoliczności, za które odpowiada Wykonawca.
   - 0,2% 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. Strony zastrzegają możliwość dochodzenia odszkodowania przenoszącego wartość kar umownych.

§8.
ODSTĄPIENIE OD UMOWY I WYPOWIEDZENIE

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 takim wypadku Zamawiający wyznaczy Wykonawcy dodatkowy 5-dniowy termin na wykonanie zobowiązania. Jeśli Wykonawca nie rozpocznie w ww. terminie wykonywania przedmiotu umowy w sposób należyty, Zamawiający ma prawo wypowiedzieć umowę ze skutkiem na dzień złożenia wypowiedzenia,
   2) naruszył bezpieczeństwo informacji lub zasady z nim związane.
3. W przypadku zwłoki w realizacji przedmiotu Umowy przekraczającej 7 dni ponad termin wskazany w §2 ust. 1 Zamawiający może, niezależnie od nałożenia na Wykonawcę kar umownych, odstąpić od umowy w całości lub

w części. Termin ten ulega odpowiedniemu przesunięciu o czas trwania opóźnień, które wynikły z winy Zamawiającego.

4. Oświadczenie o odstąpieniu lub wypowiedzeniu powinno być złożone na piśmie i zostać dostarczone drugiej Stronie.
5. Zamawiający może odstąpić od Umowy w terminie 30 dni od daty zaistnienia zdarzenia stanowiącego podstawę do odstąpienia.
6. Odstąpienie od umowy nie wpływa na obowiązek zachowania poufności informacji.
7. W razie odstąpienia od umowy lub jej wypowiedzenia, Zamawiający – w ramach należnego Wykonawcy wynagrodzenia - nabywa autorskie prawa majątkowe i zależne prawa autorskich do utworów oraz utworów i ich nośników, odnośnie do których Zamawiający praw nie nabył, w zakresie określonym w §9, z chwilą złożenia oświadczenia o odstąpieniu lub wypowiedzeniu.
8. 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 (3) tygodni, Strony spotkają się i w dobrej wierze rozpatrzą celowość i warunki rozwiązania umowy.

§9.
PRAWA AUTORSKIE

1. Wykonawca oświadcza, że będą mu przysługiwały autorskie prawa majątkowe i prawa zależne do wszelkich utworów, które powstaną w wyniku wykonania Umowy.
2. Wykonawca, z dniem podpisania protokołu odbioru Raportu, przenosi na Zamawiającego autorskie prawa majątkowe do Raportu, na następujących polach eksploatacji:
   1) w zakresie utrwalania i zwielokrotniania Raportu, - wytwarzanie określoną techniką egzemplarzy, w tym drukarską reprograficzną, elektroniczną, fotograficzną, cyfrową, audiowizualną, technikami multimedialnymi oraz zapisu magnetycznego obejmujące trwałe lub czasowe utrwalanie lub zwielokrotnianie w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu bez ograniczeń co do ilości egzemplarzy oraz korzystania i rozporządzania tymi egzemplarzami;
   2) w zakresie obrotu oryginałem albo egzemplarzami, na których Raportu utrwalono - wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
   3) w zakresie rozpowszechniania Raportu, w sposób inny niż określony w pkt 2 - publiczne wykonanie, wyświetlenie, odtworzenie, nadanie i reemitowanie, a także publiczne udostępnienie Raportu, w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym.
3. Wykonawca przenosi na rzecz Zamawiającego, z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, prawo zezwalania na wykonanie zależnego prawa autorskiego, w tym do rozporządzania i korzystania z opracowań Raportu, w nieograniczonym zakresie, w szczególności w zakresie pól eksploatacyjnych wskazanych w ust. 2.
4. Z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, Zamawiający nabywa na własność egzemplarze Raportu, przekazane przez Wykonawcę oraz nośniki, na których Raport utrwalono.
5. Zamawiający nie ponosi odpowiedzialności za naruszenie autorskich praw majątkowych lub osobistych wobec osób trzecich. Wykonawca zobowiązuje się do nieodwołalnego i bezwarunkowego zwolnienia Zamawiającego,

na pierwsze żądanie, z wszelkich roszczeń, wynikających z naruszenia majątkowych i osobistych praw autorskich, do którego doszło z przyczyn leżących po stronie Wykonawcy.

6. Wykonawca oświadcza, że przygotowany przez niego Raport będzie oryginalny i nie będzie naruszał praw osób trzecich oraz będzie wolny od wad. Wykonawca zobowiązuje się, że w momencie przekazywania Raportu Zamawiającemu będzie wyłącznym ich dysponentem majątkowym praw autorskich.
7. Przeniesienie autorskich praw majątkowych zostaje dokonane na czas nieokreślony i jest nieograniczone terytorialnie.
8. W przypadku ujawnienia nowego pola eksploatacji mającego znaczenie dla Zamawiającego, Strony ustalają, że Wykonawca na wezwanie Zamawiającego przeniesie na Zamawiającego, w terminie 14 dni od doręczenia Wykonawcy wezwania, autorskie prawa majątkowego do Raportu oraz prawo zezwalania na wykonywanie praw zależnych do Raportu na nowym polu eksploatacji, na zasadach określonych w niniejszej umowie. Przeniesienie praw, o których mowa w zdaniu poprzednim, zostanie dokonane na rzecz Zamawiającego w ramach wynagrodzenia przewidzianego niniejszą umową.

§10.
ROZSTRZYGANIE SPORÓW

1. 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.
OCHRONA INFORMACJI

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, którego wzór stanowi Załącznik nr 3 do Umowy. 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:
    3) telefonicznie, na numer telefonu: _____ .
    4) 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:
    3) zapewnić kontrolę nad tym, jakie informacje, kiedy, przez kogo oraz komu są przekazywane;
    4) 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.
ZMIANY DO UMOWY

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.
POSTANOWIENIA KOŃCOWE

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.

WYKONAWCA: **ZAMAWIAJĄCY:**

Spis załączników:
Załącznik nr 1 – Opis przedmiotu zamówienia,
Załącznik nr 2 – Oferta Wykonawcy,

Załącznik nr 7

WZÓR FORMULARZA CENOWEGO

ZADANIE NR ___								
Lp.	**Przedmiot zamówienia**	**J.m.**	**Ilość**	**Cena jednostki netto**	**Wartość netto**	**Stawka VAT**	**Wartość brutto**	**producent / nr katalogowy**
1.								
2.								
3.								
4.								
5.								
6.								
				Razem:				