[26.09.2022r.]

ZZOZ
WADOWICE

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Postępowanie o udzielenie zamówienia publicznego prowadzonego

w trybie podstawowym pod nazwą

„Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach”

Przedmiotowe postępowanie prowadzone jest przy użyciu środków komunikacji elektronicznej. Składanie ofert następuje za pośrednictwem platformy zakupowej dostępnej pod adresem internetowym: www.platformazakupowa.pl/pn/zzozwadowice

Zamawiający:
Zespół Zakładów Opieki Zdrowotnej w Wadowicach
ul. Karmelicka 5
34 – 100 Wadowice
Adres strony internetowej Zamawiającego: www.zzozwadowice.pl
e-mail: zp@zzozwadowice.pl

[26.09.2022r.]

SPIS TREŚCI

[26.09.2022r.]

I. Nazwa oraz adres Zamawiającego:

Zespół Zakładów Opieki Zdrowotnej w Wadowicach
ul. Karmelicka 5; 34-100 Wadowice
tel. 33 87 21 200; 87 21 300; fax. 823 22 30
e-mail: zp@zzozwadowice.pl
adres strony internetowej: https://zzozwadowice.pl/
Godziny urzędowania: od 7.00 do 15.00

Adres strony internetowej, na której jest prowadzone postępowanie i na której będą dostępne wszelkie dokumenty związane z prowadzoną procedurą: www.platformazakupowa.pl/pn/zzozwadowice

II. Tryb udzielenia zamówienia:

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym bez przeprowadzenia negocjacji na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710 ze zm.) zwanej dalej „ustawą Pzp", w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji
2. Zamawiający przewiduje możliwość unieważnienia postępowania o udzielenie zamówienia jeżeli środki publiczne, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostaną mu przyznane.
3. Zamawiający nie przewiduje aukcji elektronicznej.
4. Zamawiający nie dopuszcza składania ofert wariantowych.
5. Zamawiający nie dopuszcza do rozliczeń w walutach obcych.
6. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
7. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
8. Zamawiający nie przewiduje:
   - odbycia przez Wykonawcę wizji lokalnej;
   - sprawdzenia przez Wykonawcę dokumentów niezbędnych do realizacji zamówienia dostępnych na miejscu u Zamawiającego.

III. Opis przedmiotu zamówienia

Kod wg Wspólnego Słownika Zamówień (CPV):
48170000-0 Pakiety oprogramowania zapewniające zgodność

1. Opis wymagań Zamawiającego określają załącznik nr 1 do SWZ
2. Przedmiot zamówienia nie został podzielony na części ze względu na:
   - wielkość przedmiotu zamówienia oraz aspekt funkcjonalny;
   - nadmierne trudności techniczne i koszty wykonania zamówienia w częściach;
   - problemy z koordynacją działań poszczególnych części zamówienia;
   - ryzyka związane z dochodzeniem roszczeń od kilku wykonawców części.
3. Zamawiający nie dopuszcza składania ofert częściowych na poszczególne pozycje.

4. Zamawiający nie przewiduje możliwości udzielenia zamówień podobnych, o których mowa w art. 214 ust. 1 pkt 7 i 8 Ustawy Pzp.

5. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.

6. Zamawiający dopuszcza udział podwykonawców w realizacji niniejszego zamówienia. W przypadku powierzenia wykonania części zamówienia Podwykonawcy, Wykonawca zobowiązany jest do wskazania w ofercie tej części zamówienia, której realizację powierzy podwykonawcy, jak również wskazać nazwę firmy podwykonawcy (tabela w formularzu ofertowym).

7. Powierzenie części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.

8. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

IV. Termin realizacji zamówienia

Czasookres trwania umowy: do dnia 30.11.2022r.

V. Warunki udziału w postępowaniu

1.O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące:

1.1. zdolności do występowania w obrocie gospodarczym:

Zamawiający nie stawia warunku w powyższym zakresie.

1.2. uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:

Zamawiający nie stawia warunku w powyższym zakresie.

1.3. sytuacji ekonomicznej lub finansowej**:**

Zamawiający nie stawia warunku w powyższym zakresie.

1.4. zdolności technicznej lub zawodowej:

1.4.1. Warunek zdolności technicznej zostanie uznany za spełniony, jeżeli:

- Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie wykonał lub wykonuje – co najmniej 2 dostaw poparte dowodami należytego ich wykonania polegające na opracowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości działania, w skład którego wchodzi kompletna dokumentacja Bezpieczeństwa Systemu Informacji i Ciągłości działania; o wartości nie mniejszej niż 40 000 PLN netto, w tym jedna dostawa zrealizowana była na rzecz podmiotu administracji publicznej i udokumentuje, że dostawa została wykonana należycie.
- Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie wykonał lub wykonuje – co najmniej 2 dostawy poparte dowodami należytego ich wykonania polegające na opracowaniu dokumentacji bezpieczeństwa informacji i ciągłości działania, w tym postępowania w sytuacjach kryzysowych w organizacji zatrudniającej nie mniej niż 150 osób i udokumentuje, że dostawa została wykonana należycie..

1.4.2. Warunek zdolności zawodowej zostanie uznany za spełniony, jeżeli Wykonawca wykaże, iż dysponuje co najmniej dwoma audytorami zatrudnionymi przy bezpośredniej realizacji zamówienia, o minimalnych poniższych kwalifikacjach i doświadczeniu niezbędnym do wykonania zadania:

- Posiadanie certyfikatu audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2021 r. poz. 514 z późn. zm.), w zakresie certyfikacji osób.
- Posiadanie certyfikatu audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz.U. z 2021 r., poz. 514 z późn. zm.), w zakresie certyfikacji osób, lub równoważny.
- Posiadanie co najmniej trzyletniej praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych, lub co najmniej dwuletniej praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymowanie się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, uważa się udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

- przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
- przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;
- przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r., poz. 2070 z późn.zm •);
- wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r.o kontroli w administracji rządowej (t.j. Dz. U. z 2020 r., poz. 224 z późn. zm.);
- wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (t.j. Dz. U. z 2020 r. poz. 1200 z późn. zm.).

2. Zamawiający może na każdym etapie postępowania uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.

3. Ocena spełnienia ww. warunków dokonana zostanie zgodnie z formułą „spełnia – nie spełnia", w oparciu o przedłożone przez Wykonawcę oświadczenia i dokumenty, o których mowa w Rozdziele VII pkt 2.

VI. Podstawy wykluczenia z postępowania

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych w art. 108 ust. 1.

2. Wykluczenie Wykonawcy następuje na odpowiedni okres wskazany w art. 111 ustawy Pzp oraz w art. 7 ust. 2 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 ustawy Pzp, jeżeli udowodni zamawiającemu, że spełnił łącznie następujące przesłanki:

3.1. naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;

3.2. wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;

3.3. podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:

a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,

b) zreorganizował personel,

c) wdrożył system sprawozdawczości i kontroli,

d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,

e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

4. Zamawiający ocenia, czy podjęte przez wykonawcę czynności, o których mowa w pkt. 3, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w pkt. 3, nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza wykonawcę.

5. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców zgodnie z art. 7. 1. Ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego tj:

Z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych wyklucza się:

- wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 (Ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego);

-wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3(Ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego);

-wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3(Ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego).

6. Wykluczenie następuje na okres trwania okoliczności określonych w pkt. 5.

7. W przypadku wykonawcy lub uczestnika konkursu wykluczonego na podstawie pkt 5, zamawiający odrzuca wniosek o dopuszczenie do udziału w postępowaniu o udzielnie zamówienia publicznego lub ofertę takiego wykonawcy lub uczestnika konkursu, nie zaprasza go do złożenia oferty wstępnej, oferty podlegającej negocjacjom, oferty dodatkowej, oferty lub oferty ostatecznej, nie zaprasza go do negocjacji lub dialogu, a także nie prowadzi z takim wykonawcą negocjacji lub dialogu, odrzuca wniosek o dopuszczenie do udziału w konkursie, nie zaprasza do złożenia pracy konkursowej lub nie przeprowadza oceny pracy konkursowej, odpowiednio do trybu stosowanego do udzielenia zamówienia publicznego oraz etapu prowadzonego postępowania o udzielenie zamówienia publicznego.
8. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia
9. Zamawiający nie przewiduje wykluczenia Wykonawcy na podstawie art. 109 ust 1 ustawy Pzp.

VII. Wykaz oświadczeń i dokumentów, potwierdzających spełnienie warunków udziału w postępowaniu oraz braku podstaw wykluczenia. (Podmiotowe środki dowodowe).

1. Zamawiający żąda podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu. Zamawiający nie będzie żądał podmiotowych środków dowodowych na potwierdzenie braku podstaw wykluczenia.
2. Oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp, stanowi dowód potwierdzający brak podstaw wykluczenia i spełnianie warunków udziału w postępowaniu na dzień składania ofert tymczasowo zastępujący wymagane przez Zamawiającego podmiotowe środki dowodowe.
3. Oświadczenie, o którym mowa w pkt 2 Wykonawca zobowiązany jest złożyć, zgodnie ze wzorem, który stanowi **załącznik nr 2 do SWZ**.
4. Zamawiający wzywa Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
5. **Podmiotowe środki dowodowe składane na wezwanie Zamawiającego.** Na potwierdzenie spełniania warunków udziału w postępowaniu:

5.1. Wykazu wykonanych dostaw, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane– sporządzonego na podstawie wzoru stanowiącego **Załącznik nr 5 do SWZ**,

Dowodów, że dostawy wymienione w wykazie zostały wykonane lub są wykonywane należycie, w tym:

- referencje bądź inne dokumenty wydane przez odbiorcę dostawy wskazanych w wykazie, o którym mowa w pkt 7.1 SWZ, w przypadku dostaw o charakterze powtarzającym się lub ciągłym, które na dzień upływu terminu składania ofert są nadal wykonywane referencje powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;
- oświadczenie Wykonawcy składającego ofertę – jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać referencji, o których mowa w punkcie powyżej;

Uwaga!! Zamawiający nie uzna jako dowodu faktur itp. dokumentów, z uwagi na fakt, iż ich treść nie potwierdza należytego wykonania zamówienia.

5.2. Wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie dostaw, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych

przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. – sporządzonego na podstawie wzoru stanowiącego **Załącznik nr 4 do SWZ**,

6. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.

7. Jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, zamawiający może w każdym czasie wezwać wykonawcę lub wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.

8. Jeżeli złożone przez Wykonawcę oświadczenie, o którym mowa w pkt. 2 lub podmiotowe środki dowodowe budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełniania przez Wykonawcę warunków udziału w postępowaniu lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.

9. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał w oświadczeniu, o którym mowa w Załączniku nr 6 do SWZ, dane umożliwiające dostęp do tych środków. W przypadku wskazania przez Wykonawcę dostępności podmiotowych środków dowodowych pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający może żądać od wykonawcy przedstawienia tłumaczenia na język polski pobranych samodzielnie przez Zamawiającego podmiotowych środków dowodowych.

10. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

11. W zakresie nie uregulowanym SWZ, zastosowanie mają przepisy Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy.

VIII. Przedmiotowe środki dowodowe

Zmawiający nie wymaga złożenia przedmiotowych środków dowodowych.

IX. Poleganie na zasobach innych podmiotów

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.

2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te zrealizują dostawy, usługi, do realizacji których te zdolności są wymagane.

3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, 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.

4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w zdaniu poprzedzającym, potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:

4.1. zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;

4.2. sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;

5. Zamawiający ocenia, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.

6. Podmiot, który zobowiązał się do udostępnienia zasobów, odpowiada solidarnie z wykonawcą, który polega na jego sytuacji finansowej i ekonomicznej, za szkodę poniesioną przez Zamawiającego powstałą w skutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiotu nie ponosi winy.

7. Jeżeli zdolności techniczne lub zawodowe, sytuacja finansowa lub ekonomiczna podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, zamawiający żąda, aby wykonawca w terminie określonym przez zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.

8. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

9. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczeniem, o którym mowa w Rozdziale VII pkt 2 SWZ 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,

Oświadczenia podmiotów udostępniających zasoby powinny być złożone w formie **elektronicznej**, lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 273 ust. 1 ustawy Pzp. Należy je przesłać zgodnie z zasadami określonymi w Rozdziale XI SWZ.

Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunki udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w Rozdziale VII pkt 2 SWZ.

X. Informacja dla Wykonawców wspólnie ubiegających się o udzielenia zamówienia (spółki cywilne/konsorcja)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.

2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, żaden z nich nie może podlegać wykluczeniu na podstawie art. 108 ust. 1 ustawy Pzp i 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, natomiast spełnianie warunków udziału w postępowaniu Wykonawcy wykazują zgodnie z Rozdziałem V pkt 1 SWZ.

3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale VII pkt 2 SWZ, składa każdy z wykonawców wspólnie ubiegający 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.

4. W przypadku, gdy spełnienie warunku opisanego:

4.1. w Rozdziale V pkt 1.2. i 1.4 SWZ wykazuje co najmniej jeden z wykonawców wspólnie ubiegających się o udzielenie zamówienia

4.2. w Rozdziale V pkt 1.2. i 1.4 SWZ wykonawcy wykazują poprzez poleganie na zdolnościach tych z wykonawców, którzy wykonają dostawy, roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.

– wykonawcy wspólnie ubiegający się o udzielenie zamówienia oświadczają, które dostawy wykonają poszczególni wykonawcy.

5. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców są oni zobowiązani na wezwanie Zamawiającego złożyć aktualne na dzień złożenia podmiotowe środki dowodowe, o których mowa w Rozdziale VII SWZ, przy czym podmiotowe środki dowodowe o których mowa w Rozdziele VII pkt 5 SWZ składa odpowiednio Wykonawca/Wykonawcy, który/którzy wykazuje/ą spełnianie warunku, w zakresie i na zasadach opisanych w Rozdziale V SWZ;

XI. Informacja o sposobie porozumiewania się Zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami

1. Osobą uprawnioną do kontaktu z Wykonawcami jest:

1.1. Katarzyna Grzybczyk - w zakresie formalnym,

1.2. Tadeusz Hebl - w zakresie merytorycznym.

2. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformazakupowa.pl pod adresem: www.platformazakupowa.pl/pn/zzozwadowice

3. W celu skrócenia czasu udzielenia odpowiedzi na pytania preferuje się, aby komunikacja między zamawiającym a wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane są w formie elektronicznej za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego".

4. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

5. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji "Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.

6. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.

7. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz.

U. z 2020r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:

7.1. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,

7.2. komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,

7.3. zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,

7.4. włączona obsługa JavaScript,

7.5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,

7.6. Platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,

7.7. Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

8. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:

8.1. akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,

8.2. zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.

9. **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl**, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego"). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.

10. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

Zalecenia:

Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z "OBWIESZCZENIEM PREZESA RADY MINISTRÓW z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".

11. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf**

12. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:

12.1. .zip

12.2. .7Z

13. Wśród formatów powszechnych a **NIE występujących** w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. **Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.**

14. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.

15. Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
16. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
17. Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
18. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
19. Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza "Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu email.
20. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
21. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
22. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
23. Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
24. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
25. Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.

XII. Wymagania dotyczące wadium

Zamawiający nie wymaga wniesienia wadium.

XIII. Termin związania ofertą

1. Wykonawca będzie związany ofertą przez okres **30 dni**, tj. do dnia 02.11.2022 r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w pkt. 1, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XIV. Opis sposobu przygotowania ofert

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem w przypadku zamówień o wartości równej lub przekraczającej progi unijne, w przypadku zamówień o wartości niższej od progów unijnych Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym. W procesie składania

oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu[1] (**opcja rekomendowana** przez **platformazakupowa.pl**).

2. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.

3. Oferta powinna być:
   3.1. sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
   3.2. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
   3.3. podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione

4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".

5. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.

6. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.

7. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem:
https://platformazakupowa.pl/strona/45-instrukcje

8. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje podlegać będzie odrzuceniu.

9. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.

10. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.

11. Zgodnie z definicją dokumentu elektronicznego z art.3 ust 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym

[1] Rozporządzenie Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych.

podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.

12. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

13. **Dokumenty składające się na ofertę:**

13.1. odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, chyba że Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych a Wykonawca w Formularzu Oferty wskazał dane umożliwiające dostęp do tych dokumentów **w odniesieniu do Wykonawcy, Wykonawcy wspólnie ubiegającego się o zamówienie, jak również w odniesieniu do podmiotów udostępniających zasoby**; *w przypadku wskazania przez Wykonawcę dostępności ww. dokumentów pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający może żądać od Wykonawcy przedstawienia tłumaczenia na język polski pobranych samodzielnie przez Zamawiającego dokumentów.*

13.2. pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy lub podmiotu udostępniającego zasoby chyba, że umocowanie do reprezentacji wynika z dokumentów, o których mowa w Rozdziale XIV pkt 13 SWZ;

13.3. pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia (np. umowa o współdziałaniu). Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy;

13.4. zobowiązania wymagane postanowieniami Rozdziału IX pkt 3 SWZ, w przypadku gdy Wykonawca polega na zdolnościach podmiotów udostępniających zasoby w celu potwierdzenia spełniania warunków udziału w postępowaniu wraz z pełnomocnictwami, jeżeli prawo do podpisania danego zobowiązania nie wynika z dokumentów, o których mowa w Rozdziale XIV pkt 13 SWZ;

13.5. oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia, o którym mowa w art. 117 ust. 4 ustawy Pzp;

13.6. formularz ofertowy, według wzoru określonego w **Załączniku nr 6 do SWZ,**

13.7. oświadczenie dotyczące przepisów sankcyjnych związanych z wojną w Ukrainie (składa: Wykonawca, każdy z Wykonawców wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby) według wzoru określonego w **Załączniku nr 3 do SWZ**,

13.8. dokumenty wskazane w Rozdziale VIII SWZ,

13.9. oświadczenie wymagane postanowieniami Rozdziału VII pkt 2, Rozdziału IX pkt 9, Rozdziału X pkt 4 SWZ.

13.10. jeżeli Wykonawca zamierza wykazać dodatkowym doświadczeniem, o którym mowa w kryterium oceny ofert „Doświadczenie" (kryterium dodatkowo punktowane - patrz Rozdział XVII SWZ) to odpowiednie dokumenty muszą zostać złożone wraz z ofertą według wzoru określonego w **Załączniku nr 4 do SWZ**

14. **Treść złożonej oferty musi odpowiadać treści Specyfikacji. Zamawiający zaleca aby przy sporządzeniu oferty, Wykonawca skorzystał z wzorów przygotowanych przez Zamawiającego.** Wykonawca może przedstawić ofertę na swoich formularzach z zastrzeżeniem, że muszą one zawierać wszystkie informacje określone przez Zamawiającego w Specyfikacji.

15. Ofertę należy sporządzić w języku polskim. Dokumenty sporządzone w języku obcym muszą być składane wraz z tłumaczeniem na język polski.

16. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

17. Oferta i załączniki do oferty pod rygorem nieważności składa się z formie *w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym,* muszą być podpisane przez upoważnionego (upoważnionych) przedstawiciela (przedstawicieli)

18. W przypadku, gdy Wykonawcę reprezentuje Pełnomocnik wraz z ofertą winno być złożone pełnomocnictwo dla tej osoby określające jego zakres. Pełnomocnictwo winno być podpisane przez osoby uprawnione do reprezentowania Wykonawcy.

Wszelkie pełnomocnictwa winny być załączone do oferty w formie oryginału lub urzędowo poświadczonego odpisu pełnomocnictwa (notarialnie – art. 97 ust. 2 ustawy z 14 lutego 1991 r. – Prawo o notariacie (tekst jednolity Dz. U. z 2020 poz. 1192 ze zm)).

XV. Miejsce oraz termin składania i otwarcia ofert

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem *www.platformazakupowa.pl/pn/zzozwadowice* w myśl Ustawy Pzp na stronie internetowej prowadzonego postępowania **do dnia 04.10.2022 godz 10:00**

1. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.

2. Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 2 ustawy Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust. 1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

3. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.

4. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

5. Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert, nie później niż następnego dnia po dniu, w którym upłynął termin składania ofert tj. **04.10.2022 godz 10:30.**

6. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.

7. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

8. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

9. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:

10.1. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;

10.2. cenach lub kosztach zawartych w ofertach.

11. Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji ,,Komunikaty" .

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

XVI. Opis sposobu obliczenia ceny

1. Zaoferowaną cenę całkowitą (brutto) należy przedstawić w Formularzu ofertowym zgodnym z wzorem stanowiącym **Załącznik nr 6 do SWZ**.

2. Cena określona w ofercie uwzględnia wszelkie koszty wynagrodzenia Wykonawcy jakie Zamawiający zapłaci z tytułu realizacji przedmiotu zamówienia.

3. Kwoty należy zaokrąglić do pełnych groszy, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 i wyższe zaokrągla się do 1 grosza (ostatnią pozostawioną cyfrę powiększa się o jednostkę), zgodnie z art. 106e ust. 11 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tekst jednolity: Dz. U. 2020 r., poz. 106 ze zm.).

4. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w PLN.

5. Sposób zapłaty i zasady rozliczenia za realizację zamówienia, określone zostały w **Załączniku nr 7 do SWZ – Projekt Umowy.**

XVII. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert

Zamawiający podczas oceny ofert kierować się będzie następującymi kryteriami:

Kryterium	Waga
Cena	60%
Doświadczenie	40%

1. Cena 60%

$$\text{Liczba punktów} = \frac{\text{Cena najniższa spośród wszystkich ofert}}{\text{Cena oferowana}} \text{ x 100 x 60 \%}$$

2. Doświadczenie 40 %

Kryterium: doświadczenie (40%) 1pkt za każde udokumentowane wdrożenie, zgodnie informacjami w Rozdziale V pkt 1.4 określonych w minimalnych wymaganiach dla Wykonawcy. Maksymalna liczba punktów do uzyskania: 4 (po dwa udokumentowane wdrożenia dla każdego z wymagań).

Oceny ofert dokona Komisja przetargowa podczas niejawnych posiedzeń, dokonując oceny ofert zgodnie z wyżej wymienionymi warunkami. Łączna liczba punktów oferty jest sumą liczby punktów przyznawanych za poszczególne kryteria (określone powyżej).

Liczba punktów przydzielona w tym kryterium poszczególnym Wykonawcom ustalona zostanie w oparciu o Wykaz dostaw/usług – część B (**Załącznik nr 4 do SWZ**), w którym Wykonawca winien wskazać wykonane/wykonywane usług objętych przedmiotem zamówienia. Dostawy/usługi wykazane w wykazie w tabeli B będą brane pod uwagę wyłącznie do oceny oferty w kryterium „Doświadczenie".

Dostawy/usługi powtórzone z tabeli A nie będą brane przez Zamawiającego do oceny ofert. Zamawiający nie będzie wzywał Wykonawców do uzupełnienia dokumentów - dowodów, potwierdzających czy wpisane w Wykaz dostaw/usługi zostały wykonane lub są wykonywane należycie, dla dodatkowych usług wskazanych. Brak załączenia przez Wykonawcę dowodów, o których mowa powyżej, spowoduje nieuwzględnienie dodatkowych/ej dostawy/usługi przy dokonywaniu oceny ofert w kryterium „doświadczenie". Ponieważ dostawy/usługi wyszczególnione w wykazie w tabeli B nie są wykazywane w celu potwierdzenia spełniania warunków udziału w postępowaniu. Tym samym dostawy/usługi wykazane w tych pozycjach muszą stanowić doświadczenie własne Wykonawcy składającego ofertę, tj. muszą być wykonane lub wykonywane samodzielnie przez Wykonawcę.

Za najkorzystniejszą ofertę Zamawiający uzna ofertę z największą ilością punktów spośród ofert nie odrzuconych oraz spośród ofert Wykonawców niewykluczonych z postępowania.

Jeżeli w postępowaniu zostaną złożone oferty, które uzyskały taką samą liczbę punktów Zamawiający wezwie Wykonawców w terminie określonym przez Zamawiającego do złożenia ofert dodatkowych. Wykonawcy składając oferty dodatkowe nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

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

1. O wyniku postępowania Zamawiający powiadomi Wykonawcę uczestniczącego w postępowaniu oraz zamieści informację na swojej stronie internetowej ***www.platformazakupowa.pl/pn/zzozwadowice***
2. Zamawiający, zawiadomi Wykonawcę (na adres poczty elektronicznej wskazany w formularzu ofertowym), którego oferta wybrana została jako najkorzystniejsza, o terminie zawarcia umowy w siedzibie Zamawiającego tj. ZZOZ w Wadowicach, ul. Karmelicka 5, 34-100 Wadowice drogą korespondencyjną. **Zamawiający zastrzega, że w przypadku zawarcia umowy drogą korespondencyjną, za dzień zawarcia umowy uważa się datę wpisaną przez Zamawiającego w komparycji umowy. Jednocześnie Zamawiający zobowiązuje się, że w dniu wysyłki oryginału umowy do Wykonawcy, prześle droga mailową skan podpisanej jednostronnie umowy, w której wskazana będzie data jej zawarcia.**
3. Zamawiający zawrze umowę w sprawie zamówienia publicznego, z zastrzeżeniem art. 577 ustawy Pzp, w terminach określonych w art. 308 ustawy Pzp.
4. Przed zawarciem umowy w sprawie zamówienia publicznego, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia są zobowiązani przedstawić Zamawiającemu umowę regulującą podstawy i zasady wspólnego ubiegania się o udzielenie zamówienia.
5. Przed zawarciem umowy w sprawie zamówienia publicznego, Wykonawca składa dla osoby podpisującej umowę, dokument potwierdzający uprawnienie osoby podpisującej do reprezentowania Wykonawcy. Powyższe nie dotyczy sytuacji, gdy Zamawiający dysponuje już odpowiednimi dokumentami złożonymi w toku Postępowania.
6. Wybrany Wykonawca jest zobowiązany do zawarcia umowy w sprawie zamówienia publicznego na warunkach określonych we Projekcie Umowy, stanowiącym **Załącznik nr 7 do SWZ**.
7. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454 i 455 Ustawy Pzp oraz wskazanym w Projekcie Umowy, stanowiącym **Załącznik nr 7 do SWZ**.

XIX. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

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

1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów Ustawy Pzp.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 Ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:

3.1. niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

3.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy;

4. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub treści SWZ na stronie internetowej.
6. Odwołanie wnosi się w terminie:

6.1. 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

6.2. 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 6.1.

7. Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 Ustawy Pzp., stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
9. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.
10. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych, zwanego dalej "sądem zamówień publicznych".
11. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 Ustawy Pzp przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe jest równoznaczne z jej wniesieniem.
12. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.

XXI. Ochrona danych osobowych

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 danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej "RODO") informujemy, że:

1 administratorem Pani/Pana danych osobowych jest Zespół Zakładów Opieki Zdrowotnej w Wadowicach

2 administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: iod@zzozwadowice.pl

3 Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie przetargu nieograniczonego.

4 odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 Ustawy Pzp.

5 Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 Ustawy Pzp. przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

6 obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach Ustawy Pzp związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.

7 w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.

8 posiada Pani/Pan:

8.1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);

8.2. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą PZP oraz nie może naruszać integralności protokołu oraz jego załączników*);

8.3. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*);

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

9 nie przysługuje Pani/Panu:

9.1. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

9.2. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

9.3. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;

10 przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

XXII. Załączniki:

Załącznik nr 1	Opis przedmiotu zamówienia
Załącznik nr 2, 2a, 2b, 3 ,	Wzory oświadczeń
Załącznik nr 4, 5	Wykazy
Załącznik nr 6	Formularz ofertowy (wzór)
Załącznik nr 7	Projekt umowy

Pełnomocnik Dyrektora
ds. Infrastruktury i Logistyki

mgr inż. Tomasz Matera

Wadowice, dnia 26.09.2022r. Zatwierdzam **.....**
(podpis Dyrektora ZZOZ w Wadowicach
lub osoby przez niego upoważnionej)

[26.09.2022r.]

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji do dnia 30.11.2022r.

Wymagania dla wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji:

Opracowanie wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), 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 (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) - jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii w skład której wchodzą następujące dokumenty:

1. Zakres Systemu Zarządzania Bezpieczeństwem Informacji (ISO 27001) i Ciągłości Działania (ISO 22301).
2. Polityka Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.
3. Cele Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.
4. Metodyka szacowania i postępowania z ryzykiem:

- Tabela szacowania ryzyka,
- Tabela postępowania z ryzykiem,
- Raport z szacowania i postępowania z ryzykiem

5. Metodyka szacowania i postępowania z ryzykiem:

- Tabela szacowania ryzyka,
- Tabela postępowania z ryzykiem.

6. Raport z szacowania i postępowania z ryzykiem.
7. Plan szkolenia i uświadamiania.
8. Procedura audytów wewnętrznych.
9. Harmonogram audytów:

- Raport z audytu wewnętrznego,
- Lista kontrolna audytu wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.

10. Protokół z przeglądu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania.
11. Procedura działań korygujących, w tym raport z działań korygujących.
12. Procedura identyfikacji wymagań prawnych i regulacyjnych, w tym wykaz wymagań prawnych i regulacyjnych.

Dokumentacja powinna być przygotowana zgodnie z wymogami przepisów:

- Polska norma: PN-EN ISO/IEC 27001:2017-06; Technika informatyczna - Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania,
- Polska norma: PN-EN ISO 22301:2020-04; Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania -- Wymagania.

Wykonawca w ramach wynagrodzenia zobowiązany jest do przeniesienia na Zamawiającego autorskich praw do wszelkiej opracowanej i wytworzonej w ramach niniejszego zamówienia dokumentacji.

Wymagania dla Audytu KSC:

Przeprowadzenie audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej (Zamawiającego) zgodnie z wymogami Ustawy o krajowym systemie cyberbezpieczeństwa, aktów powiązanych oraz szablonem sprawozdania z audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa rekomendowanym przez Ministerstwo Cyfryzacji.
Warunki i zakres przeprowadzenia audytu końcowego w zakresie sprawdzenia bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z wymaganiami Ustawy:

a) Analiza procesów przetwarzania danych wraz z analizą stanu zabezpieczeń systemowych.
b) Identyfikacja informacji i jej klasyfikacja.
c) Inwentaryzacja zasobów infrastruktury teleinformatycznej, oprogramowania i obszarów bezpiecznych,
d) Identyfikacja i analiza podatności systemów wspomagających świadczenie usługi kluczowej.

Wynikiem analizy musi być pełna lista przeskanowanych pod kątem podatności, systemów zawierająca informacje obejmujące: skanowany system operacyjny, uruchomione na nim usługi, otwarte porty komunikacyjne, listę wykrytych podatności oraz wytyczne dotyczące sposobu usunięcia wykrytych podatności. W celu wykonania powyższych czynności, Wykonawca zobowiązany jest do zapewnienia odpowiedniej licencji na system skanujący.

e) Analiza bezpieczeństwa fizycznego i środowiskowego dla zabezpieczenia realizacji usługi kluczowej.
f) Zarządzanie: ryzykiem, incydentem, podatnościami, środkami technicznymi i organizacyjnymi, systemem monitorowania w trybie ciągłym.
g) Inwentaryzacja procedur.
h) Bezpieczeństwo i ciągłość dostaw i usług od których zależy świadczenie usługi kluczowej.
i) Przegląd dokumentacji związanej z cyberbezpieczeństwem.
j) Zidentyfikowaniu wszelkich niezgodności i wdrożenie działań naprawczych.

Audyt będzie się opierać na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby w wybranych lokalizacjach Zamawiającego oraz z wykorzystaniem zdalnego dostępu. Ponadto analiza oparta będzie o wywiad i oświadczenia wskazanych przez Zamawiającego osób.
Audyt bezpieczeństwa, może być przeprowadzony przez:

- jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2022 r. poz. 5 z późn. zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
- co najmniej dwóch audytorów posiadających:
    - certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
    - co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
    - co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
- Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z ofertą w/w certyfikatów.

Wnioski wypływające z audytu powinny wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Wynikiem audytu będzie sporządzenie przez Wykonawcę raportu, w formie papierowej oraz elektronicznej, określającego konieczne działania, a także zawierającego specyfikację rozwiązań sprzętowych oraz programowych wraz z kompleksową informacją na temat ich wdrożenia i wykorzystania u Zamawiającego celem osiągnięcia zgodności z wymaganiami Ustawy.

Powyższe wytyczne, rekomendacje oraz opisy techniczne rozwiązań (wraz z szacunkową wyceną) dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych, powinny obejmować m.in.:

- utrzymania i bezpiecznej eksploatacji systemu informacyjnego,
- bezpieczeństwa fizycznego i środowiskowego, uwzględniając kontrolę dostępu,
- bezpieczeństwa oraz ciągłości dostaw i usług, od których zależy świadczenie usługi kluczowej,
- wdrażania, dokumentowania i utrzymywania planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
- objęcia systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, systemem monitorowania w trybie ciągłym,
- wdrożenia odpowiednich środków organizacyjnych wymaganych ustawą w celu świadczenia usługi kluczowej,
- wdrożenia wymaganej ustawą dokumentacji systemu cyberbezpieczeństwa.

Obszary Audytu:

a) Ocena skuteczności działania infrastruktury w zakresie urządzeń i konfiguracji w zakresie: ochrony poczty, ochrony sieci, systemów serwerowych, stacji roboczych, systemów bezpieczeństwa,
b) Zarządzanie bezpieczeństwem informacji:
   - nośniki wymienne - udokumentowany sposób postępowania,
   - zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,
   - pomieszczenie/pomieszczenia w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwozgodnie z wymogami dla Operatora Usługi Kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.
c) Monitorowanie i reagowanie na incydenty bezpieczeństwa:
   - procedury zarządzania incydentami,
   - raportowanie poziomów pokrycia scenariuszami znanych incydentów,
   - dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa,
   - monitorowanie i wykrycie incydentów bezpieczeństwa,
   - Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów.
d) Zarządzanie ciągłością działania:
   - konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa,
   - raport z przeglądów i testów odtwarzania kopii bezpieczeństwa,
   - procedury wykonywania i przechowywania kopii zapasowych,
   - strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP),
   - procedury utrzymaniowe.
e) Utrzymanie systemów informacyjnych:
   - harmonogramy skanowania podatności,
   - aktualny status realizacji postępowania z podatnościami,
   - procedury związane ze z identyfikowaniem (wykryciem) podatności,
   - współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami.
f) Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:
   - polityka bezpieczeństwa w relacjach z dostawcami,
   - standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa,
   - dostęp zdalny,
   - metody uwierzytelnienia.

<u>Wymagania dla usługi szkoleń z zakresu cyberbezpieczeństwa</u>

Minimalne wymagania dla programu szkolenia:

• Badanie potrzeb szkoleniowych uczestników - pretest,
• Dane medyczne i osobowe— kontekst i ryzyka przetwarzanie,
• Zasady postępowania z danymi szczególnie wrażliwymi,
• Zgłaszanie incydentów dot. wycieku danych medycznych i osobowych,

• Przykłady ataków hakerskich na szpitale i placówki ochrony zdrowia,
• Czym jest cyberbezpieczeństwo,
• Metody nieautoryzowanego pozyskania danych wraz z przykładami,
• Zagrożenia w sieci (w tym phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa) wraz z przykładami,
• Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, oraz wewnętrzna bezpieczna komunikacja,
• Bezpieczne hasła, managery haseł, autoryzacja dwuetapowa, klucze sprzętowe,
• Metody obrony oraz przeciwdziałania w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, programowaniem mogącym zablokować dostęp do urządzeń firmowych, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste,
• Bezpieczne korzystanie z mediów społecznościowych,
• Bezpieczne korzystanie ze smartfonów,
• Wskazanie miejsc organizacji, oraz informacji, które należy chronić, by zniwelować ryzyko narażenia firmy na straty finansowe,
• Wskazanie zasad cyberhigieny,
• Ewaluacja szkolenia - posttest.

W ramach szkolenia zostaną zorganizowane konsultacje z kadrą zarządzającą. Tematem dyskusji będzie kontekst cyberbezpieczeństwa i prewencji w jednostkach ochrony zdrowia oraz tematyka zarządzania zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle 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 (Dz. U. z 2017 r. poz. 2247).

Minimalny czas trwania szkolenia i konsultacji 3 dni. Szkolenie przewidziane dla liczby minimum 30 uczestników. Szkolenie powinno zostać zrealizowane w formie stacjonarnej lub w szczególnym przypadku (np. wystąpienie uwarunkowań epidemiologicznych) w formie online za wcześniejszą zgodą Zamawiającego.

<u>Wymagania dla systemu Skanów Podatności:</u>

Wykonanie testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami.

W ramach przyszłej realizacji Przedmiotu Umowy zostaną wykonane następujące badania bezpieczeństwa, zgodnie z poniższym opisem

- Identyfikacja i analiza podatności systemów wspomagających świadczenie usługi kluczowej.

Wynikiem analizy musi być pełna lista przeskanowanych pod kątem podatności, systemów zawierająca informacje obejmujące: skanowany system operacyjny, uruchomione na nim usługi, otwarte porty komunikacyjne, listę wykrytych podatności oraz wytyczne dotyczące sposobu usunięcia wykrytych podatności. W celu wykonania powyższych czynności, Wykonawca zobowiązany jest do zapewnienia odpowiedniej licencji na system skanujący. W przypadku tego typu badania nie występuje próba wykorzystania wykrytych podatności, w celu uzyskania dostępu do testowanych systemów.

Usługa powinna zostać zrealizowana zgodnie z Zarządzeniem Prezesa NFZ z 20 maja. Wykonanie usługi skanów podatności, w zakresie sprecyzowanym w materiale referencyjnym „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia", opublikowanym na stronie internetowej Centrum e- zdrowia, przez okres do dnia 31 grudnia 2022 r.;

Usługa skanów podatności powinna:
- obejmować przeprowadzenie minimum jednego skanu miesięcznie, przez cały okres obowiązywania Usługi,
- po każdym przeprowadzonym skanie podatności powinien zostać sporządzony i przekazany Zamawiającemu raport z opisem podatności i rekomendacjami,
- usługa powinna zostać dostarczona w formie licencji na okres 5 lat z możliwością opłacenia całego okresu „z góry",
- Wykonawca powinien zapewnić odpowiednią licencję na system skanujący.

<u>Minimalne wymaganie dla zastosowanego systemu monitorowania:</u>

a. Automatyzacja analizy zdarzeń w systemach operacyjnych Microsoft pod kątem identyfikowania zagrożeń i incydentów bezpieczeństwa IT – system musi rozpoznawać zagrożenia wynikające z niestosowania dobrych praktyk w obszarze zarządzania kontami uprzywilejowanymi (np. zagrożenie ujawnienia hasła zapisanego w pliku tekstowym) oraz w zakresie praktyk stosowanych przez użytkowników (np. zagrożenie wykorzystania konta imiennego przez wielu pracowników).
b. System musi zapewniać ochronę użytkownika poprzez blokowanie komunikacji z źródłami zagrożeń wskazanymi przez platformę N6 CERT Polska.
c. System musi umożliwiać zarządzanie podatnościami informatycznymi. Zarządzanie należy interpretować jako funkcjonalność systemu zadaniowego, w którym to menager może wybierać i przypisywać do realizacji operatorom podatności do usunięcia. System powinien także automatyzować tworzenie zadań, jeśli nie zostanie to zrobione w sposób manualny.
d. System powinien analizować pełen kontekst procesu zarządzania bezpieczeństwem IT i w zależności od roli w organizacji, odpowiednio transformować i prezentować informacje odbiorcy. Jako minimum, role w systemie powinny być dwie: 1) Administrator usług IT, dla którego prezentowane są informacje techniczne, umożliwiające reagowanie i usuwanie zagrożenia w środowisku IT; 2) Właściciel Biznesowy usług IT w organizacji (Zarząd), dla którego prezentowane są informacje zarządcze, np. o efektywności procesu zarządzania bezpieczeństwem IT.
e. Samodzielna ocena dojrzałości organizacyjnej w zakresie zarządzania bezpieczeństwem IT. System musi umożliwiać wykonanie samodzielnego audytu w celu identyfikacji słabości organizacyjnych oraz procesowych w odniesieniu do stosowanych w tym zakresie rynkowych praktyk.
f. System musi umożliwiać wybór standardu, normy bądź innego wymogu formalno-prawnego, wobec którego będzie dokonywał oceny zgodności organizacyjnej.
g. System musi umożliwiać tworzenie własnego zakresu audytu, np. na potrzebę weryfikowania zgodności dostawców, z którymi organizacja ma podpisaną umowę.
h. System musi proponować rekomendacje do wskazanych nieprawidłowości.
i. System musi umożliwiać nadzór nad wdrażaniem działań naprawczych do zaobserwowanych nieprawidłowości.
j. System musi posiadać mechanizm tworzenia raportów czytelnie wskazujących jakie obszary były audytowane, jakie rekomendacje zostały wskazane oraz jaki jest status prac nad ich wdrożeniem.

k. System musi umożliwiać bezpieczną autoryzację użytkownika poprzez wieloskładnikowe uwierzytelnianie (bądź zapewnić możliwość integracji z zewnętrznymi systemami autoryzacji MFA).

Integracje:

a. System musi zapewniać stały dostęp do informacji o zagrożeniach w polskiej sieci Internet publikowanych poprzez z integrację z platformą N6 CERT Polska.
b. System musi posiadać moduł alarmowania o wybranych incydentach oraz zagrożeniach bezpieczeństwa IT. System powinien posiadać możliwość integracji z wybranymi operatorami bramek sms.

Pozostałe:

a. System musi być utworzony i rozwijany przez firmę polską.

Log Management

Log Management w swojej podstawowej funkcji jest centralnym punktem zbierania dowolnych danych ze środowiska IT. Baza danych oparta o silnik Elastic search zapewnia nieograniczone i wydajne gromadzenie dowolnej ilości danych, bez ograniczeń co do liczby zdarzeń, gigabajtów dziennie czy liczby źródeł danych. Kilkadziesiąt gotowych integracji oraz wprowadzona standaryzacja danych zapewniają szybki proces wdrożenia.
Jego elastyczność sprawia, że doskonale sprawdza się zarówno w dużych środowiskach, jak i małych organizacjach, oferując szybkie rezultaty od samego początku.

Log Management dostarcza niezbędnych narzędzi do zarządzania danymi. Łączy w sobie doskonałe możliwości zbierania i identyfikacji danych z precyzyjnym systemem autoryzacji, efektywnymi wizualizacjami oraz funkcjonalnością alarmowania o zdarzeniach. Wszystko to zapewnia nieograniczone możliwości zastosowania dla każdego działu IT przy wykorzystaniu jednej platformy.

Główne cechy:

KONTROLA DOSTĘPU

Pełna kontrola uprawnień dla użytkowników w dostępie do zgromadzonych danych i funkcjonalności platformy

ALERTOWANIE

Automatyczne alarmowanie o incydentach bezpieczeństwa

ARCHIWUM

Zintegrowane narzędzia umożliwiające pełne zarządzanie cyklem życia danych

WIZUALIZACJE

Bardzo bogaty zestaw wizualizacji danych

AUDYT

Szczegółowe rejestrowanie aktywności użytkowników

RAPORT

Szybkie tworzenie szczegółowych raportów

CENTRALNE ZARZĄDZANIE AGENTAMI

Łatwe zarządzanie agentami z poziomu GUI

WYSZUKIWANIE

Efektywne i szybkie wyszukiwanie danych nawet w zbiorach sięgających milionów dokumentów

Wymagania dla systemu kontroli dostępu do sieci (NAC)

Podstawowa funkcjonalność:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 500 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 5000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    a. VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
    b. Maszyny fizyczne - serwery wspierane przez producenta.
    c. Platform as a Service - Microsoft Azure.
11. System musi posiadać funkcjonalność serwerów:
    a. serwera RADIUS dla infrastruktury sieciowej,
    b. serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    c. serwera VPN,
    d. serwera DNS,
    e. serwera SYSLOG,
    f. serwera TFTP,
    g. serwera TACACS+,
    h. serwera Monitoringu,
    i. serwera DHCP,
    j. serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    k. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.

13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z minimum systemów zewnętrznych:
    a. AirWatch
    b. IBM MaaS
    c. MobileIron
    d. Microsoft Intune
    e. Google G Suite
    f. Famoc
    g. Microsoft Active Directory
    h. Radius
    i. OpenLDAP
    j. relacyjnych baz danych: MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC
    k. CheckPoint
    l. Service Now
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, konfiguracji VPN, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory minimum:
    a. Login
    b. Hasło
    c. Imię
    d. Nazwisko
    e. Email
    f. Status
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).

24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System posiada identyfikacji urządzeń końcowych z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520.
26. System musi posiadać mechanizm podglądu, tworzenia map graficznych umiejscowienia urządzeń sieciowych, końcowych, gniazdek internetowych z podziałem na budynki, pokoje oraz węzły sieciowe.
27. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
28. System musi zapewniać scentralizowane zarządzanie urządzeniami sieciowymi. Zarządzanie musi odbywać się bezagentowo, a w systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
29. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
30. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
31. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu:
    a. VLANów,
    b. Autoryzacji,
    c. Statusu,
    d. Opisu.
32. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
33. System musi zapewniać funkcjonalność wizualizacji konfiguracji podsieci IP oraz przypisania jej do jednostek.
34. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
35. System musi wspierać funkcjonalność włączania i wyłączania podsieci IP, adresów IP bez konieczności usuwania ich z systemu.
36. System musi posiadać funkcjonalność migracji sieci do sieci o większej masce wraz z dotychczasową konfiguracją sieci i ustalonymi powiązaniami adresów IP, MAC oraz konfiguracją serwera DHCP.
37. System musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja zainstalowanego oprogramowania (firmware), numer faktury zakupu, przypisane gwarancje wraz z powiadamianiem o zbliżającym się ich końcu.
38. System musi umożliwiać obsługę zdarzeń serwisowych, gwarancyjnych, reklamacyjnych urządzeń sieciowych oraz użytkownika min. rejestrowanie zdarzeń, zmianę statusu urządzenia.
39. System musi mieć możliwość oddelegowania wykonania zadań, mapowania ich z tożsamościami użytkowników, urządzeniami sieciowymi oraz urządzeniami końcowymi.
40. System musi posiadać funkcjonalność przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń sieciowych (min. w formacie tekstowym) oraz ich składowania na wewnętrznym serwerze TFTP.
41. System musi być wyposażony w funkcjonalność inwentaryzacji urządzeń w zakresie: umów, licencji, gwarancji, dostawców.

42. System musi posiadać funkcjonalność tworzenia kodów identyfikujących dla urządzeń (min. typu Barcode i QR Code) oraz ich wydruk w formacie obsługiwanym przez drukarki etykiet min. Zebra w formacie ZPL.
43. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
44. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
45. System musi posiadać mechanizm automatyzacji wg harmonogramu z możliwością symulacji działania, min:
    a. Włączenie wskazanych portów urządzeń sieciowych,
    b. Wyłączenie wskazanych portów urządzeń sieciowych,
    c. Wykonania komend na wskazanych urządzeń sieciowych,
    d. Dodanie znalezionych urządzeń sieciowych w skazanych podsieciach z możliwością sklonowania konfiguracji z podanego urządzenia sieciowego wg podanych parametrów jak: parametry dostępowe SNMP w wersji 1, 2c, 3, producenta, modelu urządzenia.
46. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.
47. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
48. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
49. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google.
50. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS.
51. System musi posiadać funkcję personalizacji strony gościnnej.
52. Captive Portal musi umożliwiać obsługę instalacji agentów, dystrybucji certyfikatów użytkowników oraz generowania autokonfiguratorów sieci.
53. System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia, pobierać certyfikaty, agenty oraz uruchamiać autokonfiguratorów sieci.
54. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
55. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
56. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS.
57. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
58. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
59. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
60. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
61. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
62. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
63. Captive Portal powinien umożliwiać podgląd ostatnich 10 logowań do sieci.
64. Captive Portal powinien umożliwiać zmianę konfiguracji numeru portów HTTP i HTTPS.

65. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
66. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
67. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
68. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego, co najmniej:
    a. Palo Alto
    b. Fortigate
    c. Sophos
    d. FlowMon
    e. ESET NOD32
    f. CheckPoint
69. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
70. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
71. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
72. System musi obsługiwać metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej:
    a. DHCP Fingerprinting
    b. DHCP SPAN
    c. SNMP
    d. Vendor OUI
    e. TCP
    f. Active Directory
    g. CDP/LLDP
    h. HTTP/S
    i. DNS
    j. Radius
    k. WMI
    l. MDM
    m. WinRM
    n. ONVIF
73. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM co najmniej:
    a. AirWatch
    b. IBM MaaS
    c. MobileIron
    d. Microsoft Intune
    e. Google G Suite
    f. Famoc

74. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach:
    a. FortiGate
    b. Pulse Secure
    c. OpenVPN
    d. Palo Alto
    e. Cisco ASA
75. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    a. Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    b. Czy włączony jest firewall
    c. Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    d. Czy jest włączone szyfrowanie dysku systemowego
    e. Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    f. Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
    g. Czy w systemie są uruchomione procesy wskazane przez administratora
    h. Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
    i. Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
        i. Wartości klucza rejestru
        ii. Typu wartości: Number, String, Version
76. System musi posiadać obsługę realizowaną przez dedykowanego agenta przełączanie VLANów na określonych portach urządzeń sieciowych.
77. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
78. System musi współpracować z serwerem tokenów.
79. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    a. Microsoft Windows
    b. Mac OS
    c. iOS
    d. Android
80. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
81. System musi umożliwiać wsparcie dla systemów typu HOT-SPOT oraz serwisami umożliwiającym oferowanie materiałów promocyjnych.
82. System musi posiadać wbudowany skaner sieciowy umożliwiający co najmniej weryfikacje otwartych portów urządzenia końcowego oraz zainstalowany system operacyjny.
83. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
    a. MAC,
    b. PAP/ASCII,
    c. CHAP,
    d. SNMP,
    e. 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
    a. Tożsamość/Urządzenie końcowe,
    b. Grupa tożsamości/urządzeń końcowych,
    c. Parametry urządzeń końcowych, min: system operacyjny, wersja,
    d. Atrybuty Active Directory,
    e. Jednostka organizacyjna tożsamości/urządzeń końcowych,
    f. Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
    g. Grupy urządzeń sieciowych,
    h. Porty urządzeń sieciowych,
    i. Grupy portów urządzeń sieciowych,
    j. Jednostka organizacyjna portów,
    k. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
    l. Data, czas ważności polityki,
    m. Wewnętrzny Captive Portal,
    n. Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów:
    a. Cisco Networks
    b. Aruba Networks
    c. Extreme Networks
    d. Hewlett Packard Enterprise
    e. Juniper Networks
    f. Ruckus Networks
    g. MicroTik
    h. Ubiquiti Networks
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi umożliwiać automatyczną konfigurację parametrów dostępowych do serwerów VPN z poziomu tożsamości.
17. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
18. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
19. System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.
20. System musi umożliwiać automatyczną generację certyfikatów z poziomu tożsamości i urządzeń końcowych.
21. System musi posiadać funkcjonalność testowania poprawności polityk z poziomu interfejsu graficznego dla wybranych tożsamości bądź urządzeń końcowych wraz z informacją zwrotną, za pomocą, której polityki zostanie przydzielony dostęp do sieci.
22. System musi wspierać funkcjonalność różnych typu autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
23. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
24. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    a. możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    b. możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    c. Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).

d. usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów VPN

1. System musi posiadać funkcję zintegrowanego serwera VPN oraz zapewniać współpracę z zintegrowanym oraz zewnętrznym serwerem CA,
2. System musi umożliwiać wystawianie konfiguracji klienckich, certyfikatów dla serwerów VPN.
3. System musi logować wszelkie próby autoryzacji do serwerów VPN.
4. System musi zapewniać przynajmniej następujące funkcjonalności serwera VPN:
    a. Logowanie do zasobów firmy,
    b. Obsługę OTP,
    c. Przypisanie ustalonego adresu IP.

Obsługa serwerów DNS

1. System musi posiadać funkcję zintegrowanego serwera DNS.
2. System musi umożliwiać graficzne zarządzanie serwerami DNS.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DNS:
    a. Zarządzanie strefami,
    b. Zarządzanie rekordami stref,
    c. Zatwierdzanie przez administratorów moderowanych rekordów stref,
    d. Weryfikacja konfiguracji przed instalacją,
    e. Instalacja konfiguracji na serwerach DNS.

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
    a. Uruchamianie usługi dla wybranych podsieci,
    b. Przypisanie ustalonego adresu IP dla adresu MAC.
    c. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
    d. Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
    e. Możliwość określania braku dostępu dla wybranych adresów MAC,
    f. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
    g. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
    h. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
    i. Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
    j. Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.

2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji:
    a. Top 10 uwierzytelnień pomyślnych (zaakceptowanych autoryzacji),
    b. Top 10 autoryzacji odrzuconych,
    c. Top 10 urządzeń sieciowych z największą liczbą autoryzacji,
    d. Top 10 urządzeń sieciowych z największą liczbą autoryzacji odrzuconych,
    e. Top 10 SSID z największą liczbą autoryzacji,
    f. Top 10 SSID z największą liczbą autoryzacji odrzuconych,
    g. Autoryzacje zaakceptowane w ciągu ostatnich 30 dni,
    h. Autoryzacje odrzucone w ciągu ostatnich 30 dni,
    i. Obciążenie serwera autoryzacji,
    j. Ostatnie 100 zdarzeń autoryzacji,
    k. Top 10 unikalnych urządzeń końcowych wg. tożsamości.
2. Monitoring dla zdarzeń systemowych:
    a. Ostatnie 100 zdarzeń systemowych,
    b. Top 10 zdarzenia typu error z Sysloga,
    c. Top 10 zdarzenia typu TopSeverity z Sysloga,
    d. Obciążenie serwera Syslog.
3. Monitoring dla zdarzeń DHCP:
    a. Wykorzystanie podsieci statyczne i dynamiczne,
    b. Ilość używanych adresów DHCP,
    c. Ostatnie 100 zdarzeń DHCP,
    d. Procentowe wykorzystanie serwera DHCP,
    e. Top 10 DHCP z największą liczbą przyznanych adresów,
    f. Top 10 DHCP z największą liczbą kolizji IP,
    g. Top 10 DHCP z największą liczbą odrzuconych IP,
    h. Top 10 DHCP z wykorzystaną pulą IP,
    i. Obciążenie serwera DHCP.
4. Monitoring dla tożsamości:
    a. Podział tożsamości ze względu na typ konta,
    b. Podział tożsamości ze względu na tożsamości aktywne i nieaktywne,
    c. Podział tożsamości ze względu na serwer autoryzacji,
    d. Podział tożsamości ze względu na konta, które straciły ważność,
    e. Wykorzystanie kont gościnnych z dostępem czasowym.

5. Monitoring dla urządzeń końcowych:
    a. Podział urządzeń ze względu na ich status,
    b. Podział urządzeń ze względu na ich typ,
    c. Podział urządzeń ze względu na serwer autoryzacji,
    d. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.
6. Monitoring dla urządzeń sieciowych:
    a. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.
    b. Podział urządzeń ze względu na ich typ.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
    a. Logowania, wylogowania z system w tym błędne logowania
    b. Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    a. wiadomości e-mail,
    b. Syslog,
    c. notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
    a. Ilości obsługiwanych transakcji RADIUS,
    b. Opóźnienie obsługi transkacji RADIUS,
    c. Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
    a. badanie łączności IP za pomocą ping, traceroute,
    b. tcpdump protokołów RADIUS, TACACS+,

c. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
    - nazwy użytkownika,
    - adresu MAC,
    - statusu uwierzytelnienia (udana lub nieudana),
    - powodu, jeżeli uwierzytelnienie nieudane,
    - zakresu czasowego, co do dnia, godziny i minuty,
d. wykonanie zdalnego polecenia na urządzeniu sieciowym.

Niespełnienie jakiegokolwiek parametru będzie skutkowało odrzuceniem oferty

[26.09.2022r.]

Załącznik nr 2 do SWZ

.....

.....

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

reprezentowany przez:
.....
.....
(imię i nazwisko, stanowisko/podstawa
do reprezentacji)

Oświadczenie Wykonawcy o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach”**,** prowadzonego przez Zespół Zakładów Opieki Zdrowotnej w Wadowicach, ul. Karmelicka 5; 34-100 Wadowice, oświadczam co następuje:

W związku z art. 125 ust. 1 ustawy Pzp:

1) oświadczam/-my, że ww. podmiot nie podlega wykluczeniu z postępowania na podstawie art. 108_____ *ustawy Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.); */*Należy dostosować odpowiednio/*

2) oświadczam/-my, że wobec ww. podmiotu zachodzą przesłanki wykluczenia z postępowania określone w art. _____ ustawy Pzp. Jednocześnie oświadczam, że w związku z ww. okolicznością, podjąłem środki naprawcze, o których mowa w art. 110 ustawy Pzp, tj.: _____;

3) oświadczam/-my, że ww. podmiot spełnia warunki udziału w postępowaniu określone przez Zamawiającego;*

4) oświadczam/-my, że w celu potwierdzenia spełniania warunków udziału w postępowaniu określonych przez Zamawiającego, polegam na zdolnościach następujących podmiotów udostępniających zasoby _____ /*podać nazwę podmiotu/,* w następującym zakresie: _____;/*podać zakres udostępnianych zasobów*/*

5) oświadczam/-my, że ww. podmiot udostępniający zasoby spełnia warunki udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby;**

6) oświadczam/-my, 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.

** Ten punkt wypełnia tylko Wykonawca/Wykonawca wspólnie ubiegający się o udzielenie zamówienia*

*** Ten punkt wypełnia tylko Podmiot udostępniający zasoby*

[26.09.2022r.]

Załącznik nr 2a do SWZ

PROPOZYCJA TREŚCI ZOBOWIĄZANIA PODMIOTU
do oddania do dyspozycji Wykonawcy niezbędnych zasobów na potrzeby realizacji zamówienia

UWAGA:
Zamiast niniejszego Formularza można przedstawić inne dokumenty, w szczególności:

1. *zobowiązanie podmiotu, o którym mowa w art. 118 ust. 4 ustawy Pzp sporządzone w oparciu o własny wzór*
2. *inne dokumenty stanowiące dowód, że Wykonawca realizując zamówienie będzie dysponował niezbędnymi zasobami podmiotów w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz, że stosunek łączący Wykonawcę z tymi podmiotami będzie gwarantował rzeczywisty dostęp do ich zasobów, określające 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,*

Ja/My:

_____
(imię i nazwisko osoby/-ób upoważnionej/-ch do reprezentowania Podmiotu, stanowisko (właściciel, prezes zarządu, członek zarządu, prokurent, upełnomocniony reprezentant itp.))

Działając w imieniu i na rzecz:

_____
(nazwa Podmiotu)

Zobowiązuję się do oddania nw. zasobów:

_____
(określenie zasobu)

do dyspozycji Wykonawcy:

_____
(nazwa Wykonawcy)

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach”, prowadzonego przez Zespół Zakładów Opieki Zdrowotnej w Wadowicach, ul. Karmelicka 5; 34-100 Wadowice, oświadczam co następuje:

1. udostępniam Wykonawcy ww. zasoby, w następującym zakresie:
   _____
   _____
2. sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia będzie następujący:
   _____
   _____

Zobowiązując się do udostępnienia zasobów, odpowiadam solidarnie z ww. Wykonawcą, który polega na mojej sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponoszę winy.

[26.09.2022r.]

Załącznik nr 2b do SWZ

Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia

w zakresie, o którym mowa w art. 117 ust. 4 ustawy Pzp

W związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego pn. „Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach", prowadzonego przez Zespół Zakładów Opieki Zdrowotnej w Wadowicach, ul. Karmelicka 5; 34-100 Wadowice,

Ja/My:

_____

(imię i nazwisko osoby/osób upoważnionej/-ych do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia)

w imieniu Wykonawcy:

_____

(wpisać nazwy (firmy) Wykonawców wspólnie ubiegających się o udzielenie zamówienia)

Oświadczam/-my, iż następujące roboty budowlane/usługi/dostawy* wykonają poszczególni Wykonawcy wspólnie ubiegający się o udzielenie zamówienia:

Wykonawca (nazwa): _____ wykona: _____**

Wykonawca (nazwa): _____ wykona: _____**

** dostosować odpowiednio*

*** należy dostosować do ilości Wykonawców wspólnie ubiegających się o udzielenie zamówienia*

[26.09.2022r.]

Załącznik nr 3 do SWZ

OŚWIADCZENIE

dotyczące przepisów sankcyjnych związanych z wojną w Ukrainie

W związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego w trybie podstawowym pn: „Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach", prowadzonego przez Zespół Zakładów Opieki Zdrowotnej w Wadowicach, ul. Karmelicka 5; 34-100 Wadowice,

JA/MY:

_____

(imię i nazwisko osoby/osób upoważnionej/-ych do reprezentowania)

działając w imieniu i na rzecz

_____

(nazwa Wykonawcy Wykonawcy wspólnie ubiegającego się o udzielenie zamówienia* Podmiotu udostępniającego zasoby*)*

I. W związku z 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 **OŚWIADCZAM**, że:

1) Wykonawca **jest* / nie jest*** wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo 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;
2) beneficjentem rzeczywistym Wykonawcy 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* / nie 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 ww. ustawy;
3) jednostką dominującą Wykonawcy 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* / nie 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 ww. ustawy.

** niepotrzebne skreślić*

[26.09.2022r.]

Załącznik nr 4 do SWZ

WYKAZ WYKONANYCH DOSTAW
(wzór)

Przystępując do postępowania przetargowego o udzielenie zamówienia publicznego pn. „Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach"

Nazwa Wykonawcy (ów) .....
Adres Wykonawcy (ów) .....
.....
oświadczam/y, że w okresie ostatnich trzech lat przed upływem terminu składania ofert w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy- w tym okresie, wykonałem/ liśmy następujące dostawy:

Część A – wykaz dostaw potwierdzającej spełnianie warunków udziału w postępowaniu

Lp.	Rodzaj i zakres (zakres usługi)	Wartość zamówienia brutto (zł)	Okres realizacji	Podmiot, na rzecz którego usługa była świadczona	Oświadczam/ y, że polegam/ y, na wiedzy i doświadczeniu
1.					własnym/ innych podmiotów*

Część B – wykaz dostaw punktowanych w ramach kryterium „Doświadczenie"

Lp.	Rodzaj i zakres (zakres usługi)	Wartość zamówienia brutto (zł)	Okres realizacji	Podmiot, na rzecz którego usługa była świadczona
1.				
2.				
Itd.				

Uwaga!! W części A i B należy wyszczególnić odmienne dostawy.

* *niewłaściwe skreślić*

.....
*data i podpis(y) osób(y) upoważnionej(ych) do reprezentowania Wykonawc**y***

* - *niepotrzebne skreślić*

[26.09.2022r.]

Załącznik nr 5 do SWZ

WYKAZ OSÓB SKIEROWANYCH PRZEZ WYKONAWCĘ DO REALIZACJI ZAMÓWIENIA

(wzór)

Przystępując do postępowania przetargowego o udzielenie zamówienia publicznego pn „Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w ZZOZ w Wadowicach"

przedkładamy wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, legitymujące się kwalifikacjami zawodowymi i doświadczeniem odpowiednimi do funkcji, jakie zostaną im powierzone, celem wykazania spełnienia opisanego przez Zamawiającego warunku w zakresie zdolności technicznej i zawodowej osób skierowanych przez Wykonawcę do realizacji zamówienia:

Lp.	Imię i nazwisko	Funkcja	Opis doświadczenia, potwierdzający spełnianie warunku opisanego w Rozdziale V pkt 1.4.2.	Podstawa dysponowania osobami

.....
*data i podpis(y) osób(y) upoważnionej(ych) do reprezentowania Wykonawc**y***

[26.09.2022r.]

Załącznik nr 6 do SWZ

Formularz Ofertowy (wzór)

Nazwa oraz siedziba Wykonawcy:.....

TELEFON: .....; FAX: .....

REGON: ....., NIP: .....

INTERNET: http: .....; e-mail: .....

Osoba odpowiedzialna za realizację umowy:.....
(imię nazwisko, tel. kontaktowy)

Osoba upoważniona do zawarcia umowy:.....
(imię nazwisko, stanowisko)

Niniejsza oferta dotyczy postępowania o udzielenie zamówienia publicznego znak: ZP.26.1.37.2022

1. Wartość oferty netto: ..... zł, brutto ..... zł (słownie brutto:.....).
2. **Termin realizacji: ..... (max do 30.11.2022 r.) od dnia zawarcia umowy.**
3. Liczba dostaw objętych przedmiotem zamówienia w okresie ostatnich 3 lat, zgodnie z Kryterium nr 2 „Doświadczenie" - .....* *należy wpisać ilość dodatkowych dostw.*
4. Oświadczam/y, że posiadam/y niezbędną wiedzę i doświadczenie oraz dysponuję/my potencjałem technicznym i osobami zdolnymi do wykonania zamówienia.
5. Termin płatności: 60 dni od daty dostarczenia prawidłowo wystawionej faktury do siedziby Zamawiającego VAT w formie przelewu.
6. Oświadczam, że wartość oferty jest ceną ostateczną do zapłaty z uwzględnieniem wszystkich czynników określonych w SWZ oraz w projekcie umowy.
7. Oświadczam/ y, że zapoznałem/ liśmy się z warunkami określonymi w specyfikacji warunków zamówienia oraz wyjaśnieniami i zmianami SWZ przekazanymi przez Zamawiającego i uznajemy się za związanych określonymi w nich postanowieniami i zasadami postępowania.
8. Oświadczam/ y, że w przypadku uznania mojej/ naszej oferty za najkorzystniejszą zobowiązuję/ emy się do dostarczenia przedmiotu zamówienia na warunkach zawartych w specyfikacji warunków zamówienia wraz z załączonym do niej projektem umowy oraz w złożonej ofercie.
9. Oświadczam/y, że dysponuję/emy osobami zdolnymi do wykonania zamówienia.
10. Oświadczam/y, że jesteśmy: [2]

10.1. mikroprzedsiębiorstwem*

10.2. małym przedsiębiorstwem*

10.3. średnim przedsiębiorstwem*

10.4. dużym przedsiębiorstwem*

---

2 Definicja miko, małego i średniego przedsiębiorcy znajduje się w art. 7 ust 1 pkt 1, 2, 3 ustawy z dnia 06 marca 2018r. Prawo przedsiębiorców (t.j. Dz.U. z 2021r. poz 162)

10.5. jednoosobowa działalność gospodarcza*

10.6. osoba fizyczna nieprowadząca działalności gospodarczej*

11. Wykonawca informuje, że:*

11.1. wybór oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

11.2. wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego w odniesieniu do następujących towarów ....., których dostawa będzie prowadzić do jego powstania. Wartość towaru lub usług powodująca obowiązek podatkowy u Zamawiającego to ..... zł netto.**

12. Wymienione niżej dokumenty stanowią tajemnicę przedsiębiorstwa i nie mogą być udostępniane osobom trzecim:

12.1. .....

12.2. .....

13. Oświadczam/y, że przewiduję/emy powierzenie zamówienia podwykonawcom ..... *(podać nazwę firmy podwykonawcy)* .....*(podać zakres powierzonych prac)* ..... *(podać wartość powierzanych prac (brutto))* .....*(podać % udział (brutto) w cenie oferty)*

14. Oświadczam/y, że nie przewiduję/emy powierzenia podwykonawcom realizacji części zamówienia*.

15. Oświadczam/y, że:

15.1. zostałem poinformowany zgodnie z art. 13 ust. 1 i 2 RODO[3] o przetwarzaniu moich danych osobowych na potrzeby niniejszego postępowania o udzielenie zamówienia publicznego oraz zawarcia i realizacji umowy[4]

15.2. wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego i zobowiązuję się wypełnić je wobec osób fizycznych od których dane osobowe bezpośrednio lub pośrednio pozyskam w celu zawarcia i realizacji umowy[5]

16. Informuję/emy, że Zamawiający posiada następujące aktualne oświadczenia lub dokumenty lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2020, poz 346 ze zm.)

LP	Nazwa oświadczenia lub dokumentu	Postępowanie, do którego zostało złożone oświadczenie lub dokument lub adres bezpłatnych i ogólnodostępnych baz danych
1		
2		

.....
data i podpis(y) osób(y) upoważnionej(ych) do reprezentowania Wykonawcy

3 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).

[4] Dotyczy wykonawcy, z którym zostanie zawarta umowa

[5] Dotyczy wykonawcy, z którym zostanie zawarta umowa

[17.05.2022r.]

Załącznik nr 7 do SWZ

Projekt umowy

zawarta w dniu ..... w Wadowicach pomiędzy:

Zespołem Zakładów Opieki Zdrowotnej w Wadowicach, ul. Karmelicka 5; 34-100 Wadowice; działającym na podstawie wpisu do Krajowego Rejestru Sądowego pod nr KRS 0000071327 prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XII Wydział Gospodarczy KRS, REGON: 000306466, NIP: 551-21-24-676 zwanym dalej w treści umowy, ***„Zamawiającym”*** reprezentowanym przez pełnomocnika:
Pełnomocnik Dyrektora ds. Infrastruktury i Logistyki ***Tomasz Matera***

a ..... Regon: ..... NIP: ....., zwanym w treści umowy ***„Dostawcą”***, reprezentowanym przez: ....

W rezultacie dokonania wyboru Wykonawcy w postępowaniu o zamówienie publiczne prowadzonym w trybie podstawowym na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U z 2022r, poz. 1710 ze z.), znak ZP.26.1.37.2022, strony zawierają umowę o następującej treści:

§1.

PRZEDMIOT UMOWY

1. Przedmiotem niniejszej umowy jest **wykonanie usług oraz dostaw polegających na:**
   1.1. wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji,
   1.2. przeprowadzeniu audytu spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa przez operatora usługi kluczowej,
   1.3. przeprowadzeniu szkolenia z zakresu cyberbezpieczeństwa,
   1.4. zakupie 5-letniej licencji na oprogramowanie do wykonywania cyklicznych testów podatności.
   1.5. zakupie rozwiązania typu Log Managment
   1.6. zakupie rozwiązania typu NAC tj. Systemu kontroli dostępu do sieci korporacyjnej (Network Access Control), zapewniającego pełny wgląd we wszystkie urządzenia i użytkowników.

   dla ZZOZ w Wadowicach, zwanych w dalszej części umowy łącznie „usługą”
2. Usługa, o której mowa w ust. 1, zostanie wykonana zgodnie ze złożoną ofertą cenową, stanowiącą **załącznik nr 1** do umowy, z SWZ i opisem przedmiotu zamówienia, stanowiącymi **załącznik nr 2**, które stanowią integralną część umowy.
3. Odbiór przedmiotu zamówienia zostanie potwierdzony przez upoważnionych przedstawicieli stron „protokołem odbioru”.

§2.

TERMIN REALIZACJI

1. Wykonawca wykona Przedmiot Umowy określony w §1 w terminie nieprzekraczalnym do dnia 20 listopada 2022 r, w tym:
   - Spotkanie koordynacyjne Stron i szczegółowe zaplanowanie realizacji usługi - do 7 dni roboczych od dnia zawarcia Umowy,
   - Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji - do 10 listopada 2022 roku,
   - Przeprowadzenie audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po wdrożeniu przez Zamawiającego czynności podnoszących poziom bezpieczeństwa systemów

teleinformatycznych - do 7 dni roboczych od dnia powiadomienia przez Zamawiającego Wykonawcy o gotowości do poddania się Audytowi. Powiadomienie Wykonawcy przez Zamawiającego o gotowości do poddania się Audytowi powinno nastąpić nie później niż do dnia 10 listopada 2022 r.

Sporządzenie Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego i przekazanie go Zamawiającemu - do 7 dni roboczych od dnia zakończenia Audytu.

- Przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa, zgodnie ze szczegółowym zakresem określonym w Załączniku nr 1 do Umowy - w terminie do 21 dni od dnia zawarcia Umowy.
- Zakup 5-letniej licencji na oprogramowanie do wykonywania cyklicznych testów podatności i wykonanie pierwszych testów podatności infrastruktury teleinformatycznej wraz z przygotowaniem raportu z opisem podatności i rekomendacjami - w terminie 21 dni od dnia zawarcia Umowy.
- Zakup i wdrożenie rozwiązania typu Log Managment - w terminie do 10 listopada 2022 roku.
- Zakup i wdrożenie rozwiązania typu NAC - w terminie do 10 listopada 2022 roku.

2. Terminy wykonania Przedmiotu Umowy określone w § 2 ust 1. mogą ulec odpowiedniemu przedłużeniu o czas trwania opóźnień, wynikających z okoliczności, za które odpowiedzialność ponosi Zamawiający.

§3.

WYNAGRODZENIE

1. Wartość przedmiotu umowy określa się do kwoty ..... zł netto ..... zł brutto (słownie brutto: .....),
2. Wynagrodzenie Wykonawcy jest ostateczne i obejmuje wszystkie koszty, jakie mogą powstać w związku z realizacją Przedmiotu Umowy, w tym wszelkie opłaty i podatki.
3. Podstawą do wystawienia przez Wykonawcę faktury będzie Protokół odbioru każdego z elementów wskazanych w Umowie, podpisany przez Zamawiającego bez zastrzeżeń.
4. W ramach realizacji Przedmiotu Umowy Wykonawca wystawi oddzielne faktury dla każdego z przewidzianych w Umowie Zadań, określonych w § 1.
5. Wynagrodzenie będzie płatne w terminie do 60 dni od dnia dostarczenia prawidłowo wystawionej faktury VAT do siedziby Zamawiającego
6. Jako datę zapłaty wynagrodzenia Dostawcy Strony uznają dzień wykonania przelewu przez Zamawiającego.
7. Dopuszcza się możliwość składania faktur w formie elektronicznej. Faktury w formie elektronicznej składane będą na adres e-mail faktury@zzozwadowice.pl. Każda wysłana wiadomość, do której załączona będzie Faktura, musi być podpisana elektronicznie. Podpis może być zrealizowany za pomocą Profilu Zaufanego lub Podpisu Elektronicznego, weryfikowanego ważnym, kwalifikowanym certyfikatem. Wykonawca może również dostarczyć ustrukturyzowaną fakturę elektroniczną za pośrednictwem PEF zgodnie z przepisami ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym, wówczas Wykonawca zwolniony zostaje z obowiązku dostarczenia faktury w wersji elektronicznej na wskazane adresy e-mail.

§4.

ZESPÓŁ

1. Wykonawca oświadcza, że dysponuje odpowiednim potencjałem techniczno–organizacyjnym, personelem posiadającym odpowiednie kwalifikacje oraz wiedzą i doświadczeniem pozwalającymi na należytą realizację przedmiotu Umowy.
2. Wykonawca zapewni Zespół specjalistów dedykowanych do realizacji Umowy, zgodnie z ofertą. Wymagania w zakresie Zespołu Wykonawcy oraz skład Zespołu określone są w Załączniku nr 2 do Umowy. Osoby

wyznaczone do wykonania Umowy posiadają kwalifikacje, wiedzę i doświadczenie zgodne z warunkami określonymi w Załączniku nr 2 do 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 kwalifikacjach lub doświadczeniu, jak określone w Załączniku nr 2 do Umowy. 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 lub pełniącej daną rolę, 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 zadań, dla których wymagania minimalne zostały określone w Załączniku nr 2 do 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, spełniającego wymagania określone w Załączniku nr 2 do Umowy, 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 których mowa powyżej, nie stanowi zmiany Umowy i nie wymaga sporządzenia 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, 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 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.
6. 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.
7. 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 poszczególnego etapu zamówienia 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 poszczególnych Zadań nastąpi w formie Protokołu odbioru, podpisanego przez Zamawiającego bez zastrzeżeń.
6. Za termin wykonania poszczególnego przedmiotu umowy strony uznają dzień podpisania przez Zamawiającego protokołu odbioru bez zastrzeżeń.

§7.

KARY UMOWNE

1. W razie niewykonania lub nienależytego wykonania umowy:

1.1. Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 10% niezrealizowanej wartości brutto przedmiotu umowy, w sytuacji gdy Zamawiający odstąpi od umowy z powodu okoliczności, za które odpowiada Dostawca,

1.2. Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 1 % wynagrodzenia brutto za każdy dzień zwłoki - w przypadku zwłoki w wykonaniu umowy ponad termin określony w § 2 ust. 1,

1.3. Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości do 20% wynagrodzenia brutto, o którym mowa w § 3 ust. 1 za każdy stwierdzony przypadek ujawnienia jakiejkolwiek informacji lub innego naruszenia bezpieczeństwa informacji, w okresie obowiązywania umowy, jak też w okresie 24 miesięcy po jej wygaśnięciu lub rozwiązaniu, w tym niewykonanie obowiązku określonego w § 11 ust. 12.

1.4. Wykonawca zobowiązuje się zapłaci Zamawiającemu karę umowną w wysokości 300 zł za każdy dzień zwłoki w przypadku niedokonania przez Wykonawcę na żądanie Zamawiającego zmiany członka personelu, zgodnie z warunkami określonymi w § 4 w terminie 14 dni od dnia zgłoszenia zastrzeżeń przez Zamawiającego.

1.5. Wykonawca zobowiązuje się zapłaci Zamawiającemu karę umowną w wysokości 300 zł za każdy dzień świadczenia usługi przez którąkolwiek z osób wchodzących w skład personelu, która nie spełnia wymagań określonych w Opisie Przedmiotu Zamówienia albo jej zmiana nie została zaakceptowana przez Zamawiającego.

2. Kary umowne mogą podlegać sumowaniu oraz mogą być naliczane niezależnie od siebie z tym zastrzeżeniem, że jeśli to samo działanie lub zaniechanie Stron wypełnia przesłanki do naliczenia dwóch lub więcej kar umownych wskazanych w Umowie, to druga Strona naliczy karę wyższą, nie może ona jednak nałożyć więcej niż jednej kary za to samo działanie czy zaniechanie. Kary będą naliczane za każdy przypadek naruszenia Umowy odrębnie.
3. W przypadku zaistnienia przesłanek naliczenia kary umownej, Strony wystawią notę obciążeniową z terminem płatności nie krótszym niż 7 dni.
4. Łączna wysokość kar umownych ograniczona jest do 20 % kwoty brutto określonej w § 3 ust. 1.

§8.

ODSTĄPIENIE OD UMOWY I WYPOWIEDZENIE

1. Zamawiającemu przysługuje prawo do odstąpienia od umowy w przypadku, gdy Wykonawca nie rozpoczął realizacji umowy lub przerwał jej wykonywanie i 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 Wykonawcy w realizacji przedmiotu Umowy przekraczającej 7 dni ponad termin wskazany w § 2 ust. 1 Zamawiający może, odstąpić od umowy w całości lub w części.
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 Raport 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. 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.

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 w imieniu Wykonawcy.
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 wysłanie wiadomości elektronicznej na adres mailowy Wykonawcy, wskazany w §4 ust. 8 Umowy.
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.

§11.

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, spowodowanych zmianami organizacyjnymi u Zamawiającego;
    2) zmiany zakresu realizacji Przedmiotu Umowy, w przypadku wystąpienia okoliczności powodujących, 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) będącym 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) spowodowanym 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) sposobu wykonania zobowiązania, o ile zmiana taka jest konieczna w celu prawidłowego wykonania Przedmiotu Umowy;
6) 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.

§12.

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 nie może przenieść wierzytelności na osobę trzecią bez zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności oraz zgody podmiotu tworzącego właściwego dla Zamawiającego zgodnie z art. 54 ust 5 i 6 ustawy o działalności leczniczej.
3. Wyklucza się stosowanie przez strony umowy konstrukcji prawnej, o której mowa w art. 518 kodeksu cywilnego (w szczególności Dostawca nie może zawrzeć umowy poręczenia z podmiotem trzecim) oraz wszelkich innych konstrukcji prawnych skutkujących zmianą podmiotową po stronie wierzyciela.
4. Wyklucza się udzielenie przez Wykonawcę upoważnienia, które skutkowałoby uprawnieniem podmiotu trzeciego do administrowania wierzytelnością, w tym dochodzenie wierzytelności wynikających z niniejszej umowy.
5. 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.
6. 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.

7. 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.
8. Wykonawca jest zobowiązany do niezwłocznego, pisemnego poinformowania Zamawiającego, że przedmiot Umowy wykonywany będzie przez:
   8.1 obywateli rosyjskich lub osoby fizyczne lub prawne, podmioty lub organy z siedzibą w Rosji;
   8.2 osoby prawne, podmioty lub organy, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w pkt 1.1 niniejszego ustępu; lub
   8.2 osoby fizyczne lub prawne, podmioty lub organy działające w imieniu lub pod kierunkiem podmiotu, o którym mowa w pkt 1.1 lub 1.2.
9. Zamawiający ma prawo do rozwiązania umowy w trybie natychmiastowym w przypadku powzięcia informacji, o której mowa w ust. 8.
10. Na podstawie ustawy z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Rozporządzenia Rady Ministrów z dnia 27 czerwca 2012 roku w sprawie warunków i sposobu przygotowania oraz wykorzystania podmiotów leczniczych na potrzeby obronne państwa oraz właściwości organów w tych sprawach oraz ustawy o obronie Ojczyzny z dnia 11 marca 2022 r. Wykonawca zobowiązuje się do realizacji usług na rzecz ZZOZ w Wadowicach również w czasie:

10.1. nadzwyczajnych zdarzeń w czasie pokoju,

10.2. zagrożenia bezpieczeństwa państwa,

10.3. wojny.

11. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego i Ustawy Prawo Zamówień Publicznych.
12. Ewentualne spory wynikłe na tle niniejszej umowy rozstrzygać będzie Sąd właściwy dla siedziby Zamawiającego.
13. Umowę sporządzono w 2 jednobrzmiących egzemplarzach: po jednym dla każdej ze Stron.
14. Załączniki do Umowy stanowią integralną część Umowy.

WYKONAWCA: **ZAMAWIAJĄCY:**

[17.05.2022r.]

Załącznik nr ..... do umowy nr .....

Klauzula informacyjna w zakresie przetwarzania danych reprezentantów

1. Informujemy, że Administratorem Danych jest ZZOZ w Wadowicach ul.Karmelicka 5

2. Kontakt do Administratora: ZZOZ w Wadowicach ul.Karmelicka 5, sekretariat@zzozwadowice.pl

3. Kontakt do inspektora ochrony danych: inspektor@zzozwadowice.pl

4. Administrator w toku prowadzonej działalności, może przetwarzać dane:

a. kontrahentów, w tym dostawców oraz potencjalnych dostawców;

b. wspólników, pracowników, przedstawicieli ustawowych oraz reprezentantów i pełnomocników ww. kontrahentów, w tym osób kontaktowych ujawnionych.

5. Administrator może przetwarzać dane podane bezpośrednio przez kontrahentów lub osoby występujące w ich imieniu, takie jak:

a. imię i nazwisko, nazwa kontrahenta, adres prowadzonej działalności oraz inne adresy korespondencyjne;

b. numery rejestracyjne we właściwych rejestrach;

c. dane kontaktowe (numer telefonu, adres email);

d. dane dotyczące statusu w strukturze kontrahenta (np.: funkcja, stanowisko, zakres uprawnień).

6. Ponadto Administrator może, w niezbędnym zakresie podyktowanym potrzebą weryfikacji kontrahenta, pozyskiwać dodatkowe informacje ze źródeł ogólnodostępnych, takich jak prowadzone na podstawie przepisów prawa rejestry gospodarcze i zawodowe (np. CEIDG, KRS).

7. Zgromadzone dane osobowe, o których mowa w pkt 1 będą przetwarzane na podstawie:

a. zgodnie z art. 6 ust. 1 lit. b) RODO, gdy przetwarzanie tych danych jest niezbędne dla realizacji umowy oraz wypełnienia wynikających z takiej umowy zobowiązań (np. imię i nazwisko, dane kontaktowe i rejestrowe). Podanie danych koniecznych dla związania umową lub jej realizacji i rozliczenia jest obowiązkowe. W tym celu może przetwarzać dane osobowe w okresie trwania umowy;

b. zgodnie z art. 6 ust. 1 lit. c) RODO, gdy przetwarzanie tych danych będzie niezbędne dla realizacji obowiązków wynikających z przepisów prawa. Podanie danych jest obowiązkowe, a obowiązek wynika z przepisów prawa. W tym celu Administrator może przechowywać dane w okresie trwania takiego obowiązku (np. dane zawarte w fakturach oraz dokumentach potwierdzających podejmowane czynności oraz transakcje)

c. dla realizacji uzasadnionych interesów Administratora lub osób trzecich, w sytuacji, gdy interesy takie są nadrzędne wobec interesów lub podstawowych praw i wolności osób, których dane dotyczą, zgodnie z art. 6 ust. 1 lit. f) RODO. Takimi uzasadnionymi interesami są np.:

i. prowadzenie bieżącej komunikacji i rozliczeń;

ii. prowadzenie korespondencji w zakresie podejmowanych działań gospodarczych, w tym realizacji umów i postępowań konkursowych i przetargowych;

iii. weryfikacja tożsamości osób działających na zlecenie naszych kontrahentów;

iv. ustalenie, dochodzenie i ochrona roszczeń wynikających z prowadzonej działalności oraz ochrona przed takimi roszczeniami – w czasie uwzględniającym okresy wygaśnięcia poszczególnych roszczeń.

8. Administrator może ujawnić dane osobowe:

a. podmiotom i osobom działającym na zlecenie na podstawie zawartych umów powierzenia przetwarzania danych osobowych w zakresie wsparcia prawnego, informatycznego i organizacyjnego,

b. organom państwowym, na podstawie przepisów prawa w ramach prowadzonych postępowań.

9. Przysługuje prawo dostępu do treści swoich danych, ich sprostowania oraz prawo do ich usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu oraz prawo do przenoszenia danych – w granicach określonych zgodnie z art. 15-22 RODO.

10. Każdej osobie przysługuje prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa) gdy uzna, iż przetwarzanie danych osobowych jest niezgodne z prawem.

[17.05.2022r.]

Załącznik nr 4 do Umowy nr .....

Umowa powierzenia przetwarzania danych osobowych na podstawie art. 28 RODO

zawarta w dniu ..... w Wadowicach pomiędzy:
Zespołem Zakładów Opieki Zdrowotnej w Wadowicach, ul. Karmelicka 5; 34-100 Wadowice; działającym na podstawie wpisu do Krajowego Rejestru Sądowego pod nr KRS 0000071327 prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XII Wydział Gospodarczy KRS, REGON: 000306466, NIP: 551-21-24-676 zwanym dalej w treści umowy, **„Powierzającym”** reprezentowanym przez pełnomocnika:
Pełnomocnik Dyrektora ds. Infrastruktury i Logistyki ***Tomasz Matera***
zwaną dalej Powierzającym
a

..... Regon: ..... NIP: ....., zwanym w treści umowy
„Przetwarzającym**”,** reprezentowanym przez: .....

zwanymi każdą z osobna w dalszej części Umowy „Stroną”, a łącznie „Stronami”.

Zważywszy, że:

- Przetwarzający będzie realizował czynności w zakresie serwisowania ..... na rzecz Powierzającego z zakresu określonego zawartą umową z dnia ..... **zwaną dalej Umową Główną**
- W związku z realizacją Umowy Głównej Przetwarzający będzie przetwarzał dane osobowe dotyczące pacjentów w zakresie danych wrażliwych dotyczących diagnostyki laboratoryjnej zgodnie z art. 9 RODO.

Strony niniejszym postanawiają zawrzeć Umowę powierzenia przetwarzania danych osobowych („Umowa”), *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 (Dz. Urz. UE L 2016, Nr 119, s.1) z dnia 4 maja 2016 r., **zwanego dalej – RODO** o następującej treści:

§ 1

Oświadczenia Stron

1. Powierzający powierza Przetwarzającemu do przetwarzania dane osobowe, które zgromadził zgodnie z obowiązującymi przepisami prawa.
2. Przetwarzający oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Powierzającego, w zakresie i celu określonym Umową.
3. Przetwarzający oświadcza również, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.
4. Przetwarzający oświadcza, że podejmuje wszelkie środki wymagane na mocy art. 32 RODO.

§ 2

Cel i charakter przetwarzania

1. Powierzający powierza Przetwarzającemu przetwarzanie danych osobowych jedynie w celu prawidłowej realizacji Umowy Głównej.
2. Przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.
3. Na wniosek Powierzającego lub osoby, której dane dotyczą Przetwarzający wskaże miejsca, w których przetwarza powierzone dane.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
2. Przetwarzający zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Przetwarzający oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
4. Przetwarzający zobowiązuje się do pełnego wdrożenia i stosowania przepisów RODO.
5. Przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Powierzającego.
6. Przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Powierzającemu poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
7. Przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Powierzającemu wywiązać się z obowiązków określonych w art. 32–36 RODO.
8. Po zakończeniu Umowy głównej Przetwarzający usunie dane osobowe i wszelkie kopie.

§ 4

Powiadomienie o naruszeniu ochrony danych osobowych

1. Przetwarzający zobowiązuje się zawiadomić o naruszeniu ochrony powierzonych danych osobowych.
2. Naruszeniem jest każdy incydent prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Powiadomienie nastąpi nie później niż do 24 godzin od momentu stwierdzenia naruszenia i będzie zawierać w szczególności:
    - opis naruszenia, w tym w miarę możliwości kategorię i przybliżoną liczbę osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których dane dotyczą;
    - opisywać możliwe konsekwencję naruszenia ochrony danych osobowych;
    - zastosowane praz proponowane środki w celu zaradzenia naruszenia ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;
    - informację czy naruszenie może spowodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą, wraz z oceną takiego ryzyka.

4. Powiadomienie należy przesłać na adres siedziby oraz adres poczty elektronicznej incydent@zzozwadowice.pl oraz na adres iod@zzozwadowice.pl

§ 5

Odpowiedzialność Stron

1. Powierzający ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).
2. Powyższe nie wyłącza odpowiedzialności Przetwarzającego za przetwarzanie powierzonych danych niezgodnie z umową.
3. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada niniejsza umowa, lub gdy działał poza zgodnymi z prawem instrukcjami Powierzającego lub wbrew tym instrukcjom.

§ 6

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
3. Niniejsza umowa powierzenia przetwarzania danych obowiązuje na czas trwania Umowy Głównej.

…… ……

POWIERZAJĄCY PRZETWARZAJĄCY