**Specyfikacja warunków zamówienia**

**ZAKUP WRAZ Z DOSTAWĄ OPROGRAMOWANIA, SPRZĘTU I USŁUG DLA PODNIESIENIA CYBERBEZPIECZEŃSTWA W**

**SAMODZIELNYM PUBLICZNYM ZAKŁADZIE OPIEKI ZDROWOTNEJ**

**W PUŁAWACH**

Numer sprawy: **45/230/2022**

1. **NAZWA (FIRMA) ORAZ ADRES ZAMAWIAJĄCEGO:**

**SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ w PUŁAWACH**

Samodzielny Publiczny Zakład Opieki Zdrowotnej, ul. J. Bema 1, 24-100 Puławy

Tel. 81 450 23 89

Adres strony internetowej: [www.szpitalpulawy.pl](http://www.szpitalpulawy.pl)

Adres e-mail: [zp@szpitalpulawy.pl](mailto:zp@szpitalpulawy.pl)

Adres skrzynki E-PUAP/SPZOZPULAWY/SkrytkaZP

Rodzaj Zamawiającego: Samodzielny Publiczny Zakład Opieki Zdrowotnej

Zamawiający nie dokonuje zakupu w imieniu innych instytucji zamawiających.

**II. TRYB UDZIELENIA ZAMÓWIENIA:**

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t. j. Dz. U. z 2021 r. poz. 1129 ze zm.) (zwanej dalej także „Pzp”, „ustawa Pzp”) oraz aktów wykonawczych wydanych na jej podstawie.

2. Niniejsza specyfikacja warunków zamówienia zwana jest w dalszej treści swz lub specyfikacją.

3. W sprawach nieuregulowanych w niniejszej swz stosuje się przepisy ustawy Pzp oraz aktów wykonawczych do ustawy Pzp.

**III. INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI**

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

**IV. OPIS PRZEDMIOTU ZAMÓWIENIA:**

1.Przedmiotem zamówienia jest dostawa oprogramowania, sprzętu i usług dla podniesienia cyberbezpieczeństwa w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Puławach, z podziałem na 2 zadania .

Nomenklatura wg (CPV): 48761000-0 - Pakiety oprogramowania antywirusowego

2. **Zadanie nr 1**

a) dostawa licencji systemów antywirusowych dla stacji roboczych i serwerów – centralnie zarządzanych, systemów klasy Endpoint and Response (EDR);

b) dostawa oprogramowania i sprzętu wraz z usługami wdrożenia, konfiguracji i szkoleń;

c) wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym.

**Zadanie nr 2**

a) realizacja audytów bezpieczeństwa.

3. Podane przez Zamawiającego ewentualne nazwy (znaki towarowe) mają charakter przykładowy a ich wskazanie ma na celu określenie oczekiwanego standardu, przy czym Zamawiający dopuszcza składanie ofert równoważnych w zakresie sporządzonego opisu przedmiotu zamówienia.

4. Przedmiot zamówienia określono poprzez wskazanie obiektywnych cech technicznych i jakościowych oraz standardów, dla których określenia dopuszcza się wskazanie przykładowych znaków towarowych.

5. Szczegółowy opis przedmiotu zamówienia znajduje się w Załączniku nr 4.

**V. TERMIN WYKONANIA ZAMÓWIENIA:**

Zamówienie musi zostać zrealizowane do 4 tygodni od daty zawarcia umowy.

**VI.** **INFORMACJA O SKŁADANIU OFERT CZĘŚCIOWYCH**

Zamawiający dopuszcza możliwość składania ofert częściowych.

**VII. INFORMACJA O SKŁADANIU OFERT WARIANTOWYCH**

Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

**VIII. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 7 I 8**

Zamawiający nie przewiduje możliwości udzielenia zamówienia, o którym mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.

**IX.** **PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO**

Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy, określone zostały w Załączniku nr 3 do SWZ.

**X. WARUNKI UDZIAŁU W POSTĘPOWANIU**

O udzielenie zamówienia mogą się ubiegać wykonawcy, którzy spełniają następujące warunki dotyczące:

1. zdolności do występowania w obrocie gospodarczym:

Zamawiający nie stawia warunku w ww. zakresie.

1. uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów Zamawiający nie stawia warunku w ww. zakresie
2. sytuacji ekonomicznej lub finansowej:

Zamawiający nie stawia warunku w ww. zakresie.

1. zdolności technicznej lub zawodowej:

Zamawiający nie stawia warunku w ww. zakresie.

**XI. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ:**

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym z Wykonawcami odbywa się przy użyciu mini Portalu <https://miniportal.uzp.gov.pl/>, ePUAPu <https://login.gov.pl/wps/portal> oraz poczty elektronicznej [zp@szpitalpulawy.pl](file:///C:\Users\mdzieglewska.SPZOZ\AppData\AppData\Local\Temp\zp@szpitalpulawy.pl). Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.

2. Wymagania techniczne i organizacyjne wysłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortaluoraz Regulaminie ePUAP.

3. Maksymalny rozmiar plików przesłanych za pośrednictwem dedykowanych formularzy do: złożenia, zmiany , wycofania oferty lub wniosku oraz do komunikacji wynosi 150MB.

4. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.

5. Zamawiający dopuszcza w szczególności następujący format przesyłanych danych: pdf, doc, docx, rtf, xps, odt.

6. Każdy Wykonawca ma prawo zwrócić się do Zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia. Wniosek Wykonawcy o wyjaśnienie treści SWZ powinien być skierowany przy użyciu, mini Portalu <https://miniportal.uzp.gov.pl/>, ePUAPu <https://epuap.gov.pl/portal> za pośrednictwem „Formularza do komunikacji” lub poczty email [zp@szpitalpulawy.pl](file:///C:\Users\mdzieglewska.SPZOZ\mmaczka\Desktop\PRZETARGI\KOMPUTERY_2\zp@szpitalpulawy.pl). Pytania należy przesyłać w wersji edytowalnej.

7. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz.U.2020 poz. 2452).

8. Zamawiający wyznacza następujące osoby do kontaktu z wykonawcami: Justyna Gawęda  
e-mail: [zp@szpitalpulawy.pl](mailto:zp@szpitalpulawy.pl), tel. 81 450 23 89.

9. Nie udziela się żadnych ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane do Zamawiającego pytania w sprawach wymagających zachowania pisemności postępowania, lub jednej ze wskazanych wyżej form porozumiewanie się pomiędzy Zamawiającym, a Wykonawcą.

10. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP i znak sprawy albo TED i znak sprawy lub ID postępowania i znak sprawy).

11. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną*, każda ze Stron na żądanie drugiej Strony niezwłocznie potwierdza fakt ich otrzymania.

**XII. INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. 69**

Zamawiający nie przewiduje użycia innych środków komunikacji elektronicznej ze względu na sytuacje, o których mowa w art. 65 ust. 1, art. 66 i art. 69 ustawy Pzp.

**XIII. TERMIN ZWIĄZANIA OFERTĄ**

1.Wykonawca jest związany ofertą od dnia upływu terminu składania ofert do dnia 19.11.2022 r.

2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, 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 o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego (t. j. wyrażonego przy użyciu wyrazów, cyfr lub innych znaków pisarskich, które można odczytać i powielić) oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

**XIV. WYMAGANIA DOTYCZĄCE WADIUM:**

Zamawiający nie przewiduje wadium.

**XV**. **OPIS SPOSOBU PRZYGOTOWANIA OFERT:**

1. Oferta musi być sporządzona w języku polskim, w postaci elektronicznej i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

2. Do przygotowania oferty należy wykorzystać Formularz ofertowy, którego wzór stanowi Załącznik nr 1 do SWZ.

3. Do oferty należy dołączyć:

a) W celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania – odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru;

b) Pełnomocnictwo upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik;

c) Pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia;

d) Formularz ofertowy, którego wzór stanowi Załącznik nr 1 do SWZ;

e) Oświadczenie Wykonawcy o niepodleganiu wykluczeniu z postępowania. Wzór oświadczenia o niepodleganiu wykluczeniu stanowi Załącznik nr 2 do SWZ. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepodleganiu wykluczeniu składa każdy z Wykonawców;

f) Klauzula informacyjna dotycząca przetwarzania danych osobowych stanowi Załącznik nr 5 do SWZ;

oraz następujące przedmiotowe środki dowodowe:

materiały informacyjne dotyczące przedmiotu zamówienia zgodne z opisem przedmiotu zamówienia, z których ma wynikać potwierdzenie wszystkich parametrów wyspecyfikowanych przez Zamawiającego. Uwaga! Jako materiał informacyjny nie może zostać złożony opis przedmiotu zamówienia Zamawiającego podpisany przez Wykonawcę, dokument złożony na potwierdzenie parametrów ma za zadanie potwierdzać wszelkie właściwości określone w opisie.

4. Do zaszyfrowania oferty nie jest potrzebna ani aplikacja do szyfrowania ofert, ani plik z kluczem publicznym. Cały proces szyfrowania ma miejsce na stronie [miniPortal.uzp.gov.pl](file:///C:\Users\mdzieglewska.SPZOZ\AppData\Local\Temp\jho9).

5. Sposób złożenia oferty, w tym zaszyfrowania oferty został opisany w Instrukcji użytkowania dostępnej na miniPortalu.

6. Jeżeli na ofertę składa się kilka dokumentów, Wykonawca powinien stworzyć folder, do którego przeniesie wszystkie dokumenty oferty, podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Następnie z tego folderu Wykonawca zrobi folder. zip(bez nadawania mu hasła i bez szyfrowania).

7. Oferta oraz oświadczenie o niepodleganiu wykluczeniu muszą być złożone w oryginale.

8. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (tj. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.

9. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t. j. Dz. U. z 2022 r., poz. 1233 ze zm.), które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa”. Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnieni. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 Pzp.

10. Jeżeli Wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie zgodnie z art. 107 ustawy Pzp.

11. Postanowień ust. 10 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego , oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

**XVI. TERMIN SKŁADANIA OFERT**

1. Ofertę wraz ze wszystkimi wymaganymi załącznikami należy wczytać na miniPortalu na stronie <https://miniportal.uzp.gov.pl/>, w terminie do dnia 20.10.2022 r. do godziny 8.00.

2. Wykonawca może złożyć jedną ofertę.

3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.

4. Wykonawca przed upływem terminu do składania ofert może zmienić lub wycofać ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty dostępnego na ePUAP i udostępnienia również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkowania dostępnej na miniPortalu.

5. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

**XVII. TERMIN OTWARCIA OFERT**

**1. Otwarcie ofert nastąpi w dniu 20.10.2022 r., o godzinie 8.30.**

2. Otwarcie ofert jest niejawne.

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

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

- nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte.

- cenach lub kosztach zawartych w ofertach.

5. W przypadku wystąpienia awarii system teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.

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

**XVIII. PODSTAWY WYKLUCZENIA**

1. Z postepowania o udzielenie zamówienia wyklucza się, z zastrzeżeniem art. 110 ust. 2 pzp, Wykonawcę̨:

1.1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo(art. 108 ust. 1 pkt. 1)):

* + 1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
    2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
    3. o którym mowa w art. 228–230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
    4. finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
    5. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
    6. pracy małoletnich cudzoziemców, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
    7. przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
    8. o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

– lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

1.2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1.1 (art. 108 ust. 1 pkt. 2));

1.3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności (art. 108 ust. 1 pkt. 3));

1.4. wobec którego orzeczono zakaz ubiegania się o zamówienia publiczne (art. 108 ust. 1 pkt. 4));

1.5. jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie (art. 108 ust. 1 pkt. 5));

1.6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 pzp, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia (art. 108 ust. 1 pkt. 6)).

2.1. który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

2.2. który naruszył obowiązki w dziedzinie ochrony środowiska, prawa socjalnego lub prawa pracy:

a) będącego osobą fizyczną skazanego prawomocnie za przestępstwo przeciwko środowisku, o którym mowa w rozdziale XXII Kodeksu karnego lub za przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, o którym mowa w rozdziale XXVIII Kodeksu karnego, lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego,

b) będącego osobą fizyczną prawomocnie ukaranego za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny,

c) wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z prawa ochrony środowiska, prawa pracy lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną;

2.3. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo lub ukarano za wykroczenie, o którym mowa w pkt 2 lit. a lub b;

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

2.5. który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;

2.6. jeżeli występuje konflikt interesów w rozumieniu art. 56 ust. 2, którego nie można skutecznie wyeliminować w inny sposób niż przez wykluczenie wykonawcy;

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

2.8. który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;

2.9. który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;

2.10. który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia.

3.Zamawiający informuje, że wykluczeniu z postępowania na podstawie pkt 7.6 SWZ podlegają:

1)  wykonawcy wymienieni w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 powołanej ustawy;

2)  wykonawcy, których beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile zostali wpisani na ww. listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego .;

3)  wykonawcy, których 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 Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.) albo wpisany na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

4. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

**XIX. OPIS SPOSOBU OBLICZENIA CENY:**

1.Wykonawca poda cenę oferty w Formularzu Ofertowym sporządzonym według wzoru stanowiącego Załącznik nr 1 do SWZ, jako cenę brutto (z uwzględnieniem kwoty podatku od towarów i usług (VAT)) z wyszczególnieniem stawki podatku od towarów i usług (VAT).

2. Cena oferty stanowi wynagrodzenie ryczałtowe.

3. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.

4. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nie-prawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty, jeżeli nie ziszczą się ustawowe przesłanki omyłki (na podstawie art. 226 ust. 1 pkt 10 Pzp w związku z art. 223 ust. 2 pkt 3 Pzp).

5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).

6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

**XX. INFORMACJA DOTYCZĄCA WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ:**

1. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
2. Zamawiający nie przewiduje rozliczenia w walutach obcych.

**XXI. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW, I SPOSOBU OCENY OFERT:**

**Kryteria oceny ofert i ich znaczenie dla Zadania nr: 1**

**1. Oferta będzie oceniana w oparciu o poniższe kryteria:**

**1 - Cena brutto - 60 %**

W trakcie oceny ofert kolejno rozpatrywanym i ocenianym ofertom przyznawane są punkty według:

- za najniższą cenę brutto – 60 pkt

Cena oferowana minimalna brutto

Cena = ----------------------------------------------- x 60 pkt

Cena brutto badanej ofert

**2 –** **Czas dostawy urządzeń**  **– 40%\*\***

Kryterium czasu dostawy - Kc

Najkrótszy czas dostawy w dniach

Kc = …………………………………………………………................ 40 pkt

Czas realizacji badanej oferty w dniach

\*\* Czas realizacji Zamówienie wynosi: nie dłuższy niż 14 dni roboczych od momentu podpisania umowy.

Zaoferowanie czasu dostawy dłuższego niż 14 dni spowoduje odrzucenie oferty.

**Kryteria oceny ofert i ich znaczenie dla Zadania nr: 2**

**1 - Cena brutto - 60 %**

W trakcie oceny ofert kolejno rozpatrywanym i ocenianym ofertom przyznawane są punkty według:

- za najniższą cenę brutto – 60 pkt

Cena oferowana minimalna brutto

Cena = ----------------------------------------------- x 60 pkt

Cena brutto badanej ofert

2. \***Czas realizacji audytu -** 40%

najkrótszy licząc od dnia podpisania umowy – 40 pkt

Termin wykonania zamówienia liczony w dniach (znaczenie kryterium – max. 40 pkt) będzie oceniane na podstawie wzoru:

Czas realizacji audytu w dniach

Czas realizacji audytu = ------------------------------------------------------------------ x 40 pkt

Najdłuższy czas realizacji audytu w dniach

\*\* Minimalny czas realizacji audytu 7 dni roboczych od dnia zgłoszenia gotowości audytu.

Zaoferowanie czasu realizacji audytu krótszego spowoduje, że do wzoru zostanie podstawiony termin minimalny 7 dni.

\*\* Maksymalny czas realizacji audytu 14 dni roboczych od dnia zgłoszenia gotowości audytu. Zaoferowanie czasu realizacji audytu dłuższego niż 14 dni spowoduje odrzucenie oferty.

**Za ofertę najkorzystniejszą złożoną w ramach tego przetargu zostanie uznana oferta, która uzyska największą liczbę punktów za wszystkie kryteria oceny łącznie.**

2. Zamawiający udzieli zamówienia Wykonawcy, którego oferta uzyska największą liczbę punktów.

3. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie, wezwie on Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.

4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.

5. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.

6. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.

7. W przypadku braku zgody, o której mowa w ust. 6, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania*.*

**XXII. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY, W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO:**

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego , z uwzględnieniem art. 557pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektrycznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.

2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzieleniu zamówienia złożono tylko jedną ofertę.

3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany prze Zamawiającego o miejscu i terminie podpisania umowy.

4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią Załącznik nr 3 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.

5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.

6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

**XXIII. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, OGÓLNE WARUNKI UMOWY ALBO WZÓR UMOWY (ZAŁĄCZNIK 3A, ZAŁĄCZNIK 3B), JEŻELI ZAMAWIAJĄCY WYMAGA OD WYKONAWCY, ABY ZAWARŁ Z NIM UMOWĘ W SPRAWIE ZAMÓWIENIA PUBLICZNEGO NA TAKICH WARUNKACH:**

1. Zamawiający informuje, że przewiduje możliwości zmiany umowy. Zmiany zawartej umowy mogą nastąpić w następujących przypadkach, gdy:

a) ulegnie zmianie stan prawny w zakresie dotyczącym realizowanej umowy, który spowoduje konieczność zmiany sposobu wykonania zamówienia przez Wykonawcę;

b) wystąpią przeszkody o obiektywnym charakterze (zdarzenia nadzwyczajne, zewnętrzne   
i niemożliwe do zapobieżenia, a więc mieszczące się w zakresie pojęciowym tzw. siły wyższej), np. pogoda uniemożliwiająca wykonywanie umowy, zdarzenia nieleżące po żadnej ze stron umowy. Strony mają prawo do skorygowania uzgodnionych zobowiązań i przesunięcia terminu realizacji maksymalnie o czas trwania siły wyższej. Strony zobowiązują się do natychmiastowego poinformowania się nawzajem o wystąpieniu ww. przeszkód;

c) nastąpi konieczność wykonania innych, nieprzewidzianych prac, nieuwzględnionych w opisie przedmiotu zamówienia, a niezbędnych do zrealizowania przedmiotu zamówienia skutkujących przesunięciem terminu realizacji zamówienia o czas niezbędny do ich wykonania.

2. Wzór umowy stanowi załącznik nr 3 do niniejszej swz.

3. Strony dopuszczają możliwość zmian redakcyjnych, korekty omyłek pisarskich oraz zmian będących następstwem zmian danych ujawnionych w rejestrach publicznych bez konieczności sporządzania aneksu.

4. Gdyby nastąpiła zmiana stawki podatku od towarów i usług, umowa nie ulegnie zmianie w zakresie wysokości ceny netto.

**XXIV. WSKAZANIE CZĘŚCI ZAMÓWIENIA, KTÓRA MOŻE BYĆ POWIERZONA PODWYKONAWCOM:**

Zamawiający dopuszcza wykonanie przedmiotu zamówienia przy udziale podwykonawców. Zakres prac, który Wykonawca zamierza powierzyć podwykonawcom oraz nazwy podwykonawców należy wymienić w ofercie Wykonawcy – zgodnie z załącznikiem nr 1 do swz.

W przypadku gdy Wykonawca nie wskaże powyższych informacji, Zamawiający uzna, iż zamówienie realizowane będzie bez udziału podwykonawców.

**XXV. INFORMACJA O UMOWIE RAMOWEJ:**

Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.

**XXVI. INFORMACJE DODATKOWE DOTCZACE WYSOKOŚCI ZWROTU KOSZTÓW UDZIAŁU W POSTEPOWANIU, JEŻELI ZAMAWIAJĄCY PRZEIDUJE ICH ZWROT, ORAZ AUKCJI ELEKTRONICZNEJ, JEŻELI ZAMAWIAJĄCY PRZEWIDUJE AUKCJĘ ELEKTRONICZNĄ.**

1. Wszystkie koszty związane z uczestnictwem w postępowaniu, w szczególności  
z przygotowaniem i złożeniem ofert ponosi Wykonawca składający ofertę.

2. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

3. Zamawiający nie przewiduje aukcji elektronicznej.

**XXVII. WYMAGANIA W ZAKRESIE ZATRUDNIENIA OSÓB ORAZ INFORMACJA O ZASTRZEŻENIU MOŻLIWOŚCI UBIEGANIA SIĘ O UDZIELENIE ZAMÓWIENIA WYŁĄCZNIE PRZEZ WYKONAWCÓW, O KTÓRYCH MOWA W ART. 94**

Zamawiający nie stawia wymagań.

**XXVIII. INFORMACJA DOTYCZĄCA ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY**

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

**XXIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA:**

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

2. Odwołanie przysługuje na:

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

2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.

3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.

4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.

5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” Pzp.

**XXX. ZAŁĄCZNIKI DO SWZ**

Załącznik nr 1 – Oferta wykonawcy

Załącznik nr 2 – Wzór oświadczenia o niepodleganiu wykluczeniu

Załącznik nr 3 – Projektowane postanowienia umowy

Załącznik nr 4 – Szczegółowy opis przedmiotu zamówienia

Załącznik nr 5 – Klauzula informacyjna dotycząca przetwarzania danych osobowych.

Puławy, 10.10.2022 r. podpis Zamawiającego:

**Dyrektor SP ZOZ w Puławach**

**Piotr Rybak**

**Załącznik nr 1 do SWZ**

Nazwa wykonawcy: ….....................................................................................................................

**KRS** wykonawcy: …........................................................................................................................

**NIP** wykonawcy: …...........................................................................................................................

**REGON** wykonawcy: …....................................................................................................................

adres wykonawcy: ….......................................................................................................................

kod pocztowy i miejscowość: ….......................................................................................................

województwo…..........................................................................................................................

telefon: …..........................................................

poczta elektroniczna (e-mail): …..............................................................................

adres internetowy (URL): ….....................................................................................

Nazwisko i kontakt osoby upoważnionej do kontaktów: …..............................................................

**Wykonawca jest:**

* mikroprzedsiębiorstwem,
* małym przedsiębiorstwem,
* średnim przedsiębiorstwem,
* jednoosobową działalnością gospodarczą,
* osobą fizyczną nieprowadzącą działalności gospodarczej,
* innym rodzajem\*

## O F E R T A W Y K O N A W C Y

1. Oferujemy dostawę oprogramowania, sprzętu i usług dla podniesienia cyberbezpieczeństwa w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Puławach na warunkach i zasadach określonych w swz ZM 45/230/2022 po cenie ryczałtowej zgodnej z ceną podaną w załączniku nr 4 do SWZ.

**Zadanie nr 1:**

brutto: .........................................................................................................

(cena brutto słownie: ………...............................................................................................................)

Wykonawca według powyższego wzoru wypełnia ofertę dla zadań, w których składa ofertę.

Czy wybór oferty będzie prowadził do powstania obowiązku podatkowego po stronie Zamawiającego TAK/NIE\*

Jeżeli Wykonawca wskaże TAK (powstanie obowiązek podatkowy u Zamawiającego), Wykonawca wskazuje rodzaj towaru/usługi, której ten obowiązek dotyczy ……………………………. (nazwa towaru/usługi).

Zadanie nr 1:

Cena netto (bez VAT) ……………. (Uwaga! Dotyczy tylko dostaw/usług, dla których obowiązek podatkowy przechodzi na Zamawiającego).

2.Oferujemy realizację dostawy w ciągu …… dni roboczych licząc od dnia podpisania umowy (nie dłuższy niż 14 dni roboczych).

3.Okres gwarancji urządzeń: min 36 miesięcy.

**Zadanie nr 2:**

brutto: .........................................................................................................

(cena brutto słownie: ………...............................................................................................................)

Wykonawca według powyższego wzoru wypełnia ofertę dla zadań, w których składa ofertę.

Czy wybór oferty będzie prowadził do powstania obowiązku podatkowego po stronie Zamawiającego TAK/NIE\*

Jeżeli Wykonawca wskaże TAK (powstanie obowiązek podatkowy u Zamawiającego), Wykonawca wskazuje rodzaj towaru/usługi, której ten obowiązek dotyczy ……………………………. (nazwa towaru/usługi).

Zadanie nr 2:

Cena netto (bez VAT) ……………. (Uwaga! Dotyczy tylko dostaw/usług, dla których obowiązek podatkowy przechodzi na Zamawiającego).

2. Oferujemy czas realizacji audytu w ciągu …… dni roboczych licząc od dnia zgłoszenia gotowości audytu (nie dłuższy niż 14 dni roboczych).

Adres e-mail ……………………….. do przesyłania dokumentów finansowych (np. faktury, noty).

3. Adres skrzynki ePUAP Wykonawcy: ………………

4. Termin płatności 30 dni.

5. Oświadczamy, iż zaakceptowaliśmy termin realizacji przedmiotu umowy wskazany w części V swz oraz w umowie.

6. **Oświadczamy**, że zapoznaliśmy się ze specyfikacją warunków zamówienia i akceptujemy wszystkie warunki w niej zawarte.

7. **Oświadczamy**, że uzyskaliśmy wszelkie informację niezbędne do prawidłowego przygotawania i złożenia niniejszej oferty.

8. Jesteśmy związani niniejszą ofertą na czas wskazany w specyfikacji warunków zamówienia.

9. **Oświadczamy**, że zapoznaliśmy się z Projektowanymi Postanowieniami Umowy, określonymi w Załączniku nr 3 do Specyfikacji Warunków Zamówienia i Zobowiązujemy się, w przypadku wybranej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach w nich określonych.

10. **Oświadczamy**, iż zamierzamy zlecić podwykonawcy następujące części zamówienia

(wypełnić tylko w przypadku realizacji zamówienia przy udziale podwykonawców)

część ………………………………… nazwa podwykonawcy ………………..

część ………………………………… nazwa podwykonawcy ………………..

11. **Oświadczamy**, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[[1]](#footnote-1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*\*

12. Integralną część niniejszej oferty stanowią dokumenty wymagane treścią rozdziału XIII swz.

……………………… dnia ……………………

……………………………………………………..

*(podpis osoby upoważnionej do reprezentacji)*

***Informacja dla Wykonawcy:***

*Formularz ofertowy (oraz Załączniki do niniejszego formularza) musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem(ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.*

*\*niepotrzebne skreślić*

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

**Załącznik Nr 2 do SWZ**

**Zamawiający:**

Samodzielny Publiczny Zakład Opieki Zdrowotnej Puławach

ul. Bema 1, 24-100 Puławy

*(pełna nazwa/firma, adres)*

**Wykonawca:**

…………………………………………………………………………

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

reprezentowany przez:

…………………………………………………………………………

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

**Oświadczenie wykonawcy**

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

**Prawo zamówień publicznych (dalej jako: Pzp),**

**DOTYCZĄCE PODSTAW WYKLUCZENIA Z POSTĘPOWANIA**

Na potrzeby postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest

**”DOSTAWA OPROGRAMOWANIA, SPRZĘTU I USŁUG DLA PODNIESIENIA CYBERBEZPIECZEŃSTWA W SAMODZIELNYM PUBLICZNYM ZAKŁADZIE OPIEKI ZDROWOTNEJ** ”

prowadzonego przez Samodzielny Publiczny Zakład Opieki Zdrowotnej Puławach

oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

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

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

…………………………………………

*(podpis)*

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

……………………………………………………………………………………………………………

……………………………………………………………………………………………

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

…………………………………………

*(podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:**

Oświadczam, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj. : …………………………………………………………………….…………………………

…………………………………………………………………….……………………………………  
*(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

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

…………………………………………

*(podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

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

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

…………………………………………

*(podpis)*

**Załącznik Nr 3a do SWZ**

**Umowa Nr /P/2022**

**na dostawę infrastruktury sprzętowej oraz oprogramowania**

zawarta dnia …...……….….. w Puławach, pomiędzy:

**Samodzielnym Publicznym Zakładem Opieki Zdrowotnej z siedzibą w Puławach przy ul. Bema 1,   
24-100 Puławy**, zarejestrowanym w rejestrze stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej prowadzonego przez Sąd Rejonowy Lublin - Wschód w Lublinie z siedzibą w Świdniku, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000026256, NIP 716-22-38-942, REGON 431205731

reprezentowanym przez:

- Piotra Rybaka – Dyrektora

zwanym dalej **„Zamawiającym”**

oraz

**………………………**. z siedzibą w ……………………………………………………… wpisanym do …………………………………………………………………………………….. prowadzonego przez Sąd Rejonowy dla ……………………., ……… Wydział Krajowego Rejestru Sądowego pod numerem KRS…………………….., NIP……………………….., REGON …………………...,

zwanym w dalszej części umowy **„Wykonawcą”** lub **„Stroną”**,

reprezentowanym przez:

- …………………………………

zwani łączni w dalszej części umowy **„Stronami”**,

o następującej treści:

Zamawiający i Wykonawca będą dalej łącznie zwani **„Stronami”**, a każdy z nich z osobna także **„Stroną”**.

Wobec wyboru oferty Wykonawcy jako najkorzystniejszej w przeprowadzonym przez Zamawiającego postępowaniu w sprawie udzielenia zamówienia w trybie przetargu podstawowego  
nr ZM 45/230/2022 i na warunkach określonych w SWZ na podstawie ustawy z dnia 11 września 20019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.) (dalej: ustawa Pzp) Strony postanawiają co następuje:

**§ 1**

**Przedmiot umowy**

1. Przedmiotem zamówienia jest dostawa wraz z instalacją infrastruktury sprzętowej oraz oprogramowania o parametrach minimalnych i w ilościach podanych w załącznik nr 4 do SWZ tj. zgodnych z szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 2 do Umowy.

2. Wykonawca zobowiązany jest do kompleksowej realizacji przedmiotu zamówienia zgodnie z wymaganiami niniejszej umowy oraz Załącznika nr 1 i nr 2 do umowy w taki sposób, aby zrealizowany przedmiot umowy był gotowy do użycia bez dodatkowych inwestycji Zamawiającego (tj. bez konieczności dokonywania przez Zamawiającego dodatkowych zakupów lub nabywania dodatkowych usług w zakresie przedmiotu zamówienia).

3. W celu uniknięcia wszelkich wątpliwości strony zgodnie ustalają, że dla prawidłowej realizacji przez Wykonawcę przedmiotu umowy, o którym mowa w ust. 1 i 2 powyżej, Wykonawca jest zobowiązany wykonać wszelkie dostawy i prace opisane w Szczegółowym Opisie Przedmiotu Zamówienia oraz wszelkie inne prace, czynności choćby nie zostały wyszczególnione w Szczegółowym Opisie Przedmiotu Zamówienia (takie jak montaż danego elementu na ścianie bądź uporządkowanie kabli oraz całego miejsca montażu przed i po działaniu), a są konieczne do prawidłowej realizacji przedmiotu umowy z punktu widzenia celu, któremu realizowana inwestycja ma służyć.

4. W przypadku sprzeczności pomiędzy treścią niniejszej umowy, a warunkami zawartymi w treści Załącznika nr 2 do Umowy, pierwszeństwo mają postanowienia zawarte w treści Załącznika nr 2 do Umowy.

5. Wykonawca oświadcza, że część zamówienia, tj...................................................., powierzył do realizacji podwykonawcy, .......................................... (\*w przypadku gdy tak stanowi treść oferty Wykonawcy).

**§ 2**

**Odbiór zamówienia**

1. Protokół odbiorczy przygotowany przez Wykonawcę i podpisany przez upoważnionych przedstawicieli stron stanowić będzie potwierdzenie przyjęcia przez Zamawiającego wykonanych przez Wykonawcę dostaw i prac będących przedmiotem umowy. Odbiór dostaw i prac uważa się za dokonany w przypadku podpisania protokołu odbiorczego z klauzulą „bez zastrzeżeń” przez Zamawiającego. W chwili przekazania Zamawiającemu przedmiotu umowy Strony podpiszą protokół dostawy. Ostateczny odbiór przedmiotu umowy nastąpi na podstawie końcowego protokołu, o którym mowa w ust. 2 powyżej.

2. Dokumentem potwierdzającym zakończenie realizacji umowy będzie podpisany przez upoważnionych przedstawicieli obu stron protokół końcowy z klauzulą „bez zastrzeżeń”, stanowiący podstawę do wystawienia przez Wykonawcę faktury VAT oraz dokonania przez Zamawiającego zapłaty wynagrodzenia Wykonawcy.

3. Wykonawca zawiadomi Zamawiającego o gotowości do odbioru przedmiotu umowy drogą elektroniczną na adresy osób wskazanych w ust. 11 poniżej.

4. Zamawiający wyznaczy termin odbioru w ciągu 3 dni roboczych od dnia zawiadomienia przez Wykonawcę o gotowości do odbioru. Termin ten nie powinien być późniejszy niż 3 dni od dnia zawiadomienia.

5. W przypadku stwierdzenia w trakcie odbioru jakichkolwiek nieprawidłowości wykonanych przez Wykonawcę dostaw i prac objętych przedmiotem zamówienia, w tym wad fizycznych, niezgodności z umową np. niezgodność parametrów technicznych lub eksploatacyjnych sprzętu lub oprogramowania w stosunku do wymagań umownych w szczególności zawartych w Załączniku nr 2 do umowy, brak, niedziałanie lub nienależyte działanie jakiegokolwiek elementu sprzętu lub oprogramowania, brak wymaganych umową i jej załącznikami dokumentów Zamawiający ma prawo odmówić odbioru. Zamawiający nie jest zobowiązany w takiej sytuacji do dokonania zapłaty za wadliwe sprzęty/usługę. Zamawiający będzie zobowiązany do zapłaty wynagrodzenia Wykonawcy dopiero po stwierdzeniu prawidłowego, (zgodnego z umową i załącznikami do umowy ) wykonania przez Wykonawcę przedmiotu umowy, potwierdzonego przez Zamawiającego w protokole końcowym, o którym mowa w ust. 1 powyżej.

6. W przypadku, o którym mowa w ust. 5 powyżej (tj. w przypadku stwierdzenia w trakcie odbioru niezgodności realizacji przedmiotu zamówienia z warunkami umowy wraz z załącznikami) Zamawiający sporządzi protokół zawierający listę usterek, a Wykonawca zobowiązany będzie do usunięcia na własny koszt stwierdzonych w trakcie odbioru niezgodności w terminie uzgodnionym przez Strony (nie dłuższym jednak niż 10 dni roboczych), z zastrzeżeniem, iż po bezskutecznym upływie tego terminu Zamawiający będzie mógł odstąpić od umowy z przyczyn leżących po stronie Wykonawcy, niezależnie od istotności stwierdzonych niezgodności z warunkami umowy i jej załącznikami oraz żądać zapłaty kary umownej, o której mowa w § 5 umowy.

7. W przypadku stwierdzenia w trakcie odbioru niezgodności, o których mowa w ust. 5 protokół odbiorczy, o którym mowa ust. 1 powyżej i protokół końcowy, o którym mowa w ust. 2 powyżej zostanie sporządzony po usunięciu przez Wykonawcę niezgodności wskazanych w protokole usterek.

8. Brak uczestnictwa Wykonawcy w czynnościach odbioru upoważnia Zamawiającego do dokonania odbioru bez udziału Wykonawcy, na ryzyko Wykonawcy w przypadku stwierdzenia niezgodności z umową. W takim przypadku Zamawiający może jednostronnie sporządzić i podpisać protokół odbiorczy.

9. W przypadku wykonania zamówienia, Wykonawca odpowiada za działania i zaniechania, uchybienia i zaniedbania podwykonawcy, tak jak za własne działania i zaniechania, uchybienia i zaniedbania.

10. W przypadku stwierdzenia w protokole odbioru końcowego wad, usterek lub innych braków w przedmiocie dostawy, zgłoszenie usunięcia wad, usterek lub innych braków należy przesłać pocztą elektroniczną na adres (lub adresy) wskazany w ust. 11 poniżej.

11. Ze strony Zamawiającego do wyznaczenia terminu, dokonania odbioru i innych czynności związanych z odbiorem upoważnieni są: …………………..….. (tel. …………………..), e-mail: ………, ………. (tel. ………………………..), e-mail: ……………………………………...

12. Wykonawcę w kwestiach związanych z przekazaniem przedmiotu umowy reprezentuje …………………………, tel. ………………………..., e-mail: ……………………………..…..

**§3**

**Warunki płatności**

1. Za pełne i prawidłowe wykonanie przedmiotu Umowy Wykonawca otrzyma wynagrodzenie w kwocie ………….. zł **netto** (słownie: …………………………..) plus należny podatek VAT, co stanowi kwotę **brutto** ………………. (słownie: …………………………..) i obejmuje, zgodnie z formularzem ofertowym stanowiącym Załącznik nr 1 do umowy oraz Szczegółowym opisem przedmiotu zamówienia stanowiącym Załącznik nr 2 do Umowy kompleksową realizację przedmiotu zamówienia, w tym w szczególności koszty dostawy sprzętów i oprogramowania, instalacji i uruchomienia sprzętów i oprogramowania oraz wszelkie koszty związane z zakresem usługi wdrożeniowej zgodnie z Załącznikiem nr 2 do Umowy w tym m.in. gwarancją, opieką administracyjną, szkoleniem, a także wszelkich innych czynności wymaganych dla prawidłowego wykonania umowy. Wykonawca nie będzie mógł żądać od Zamawiającego pokrycia jakichkolwiek kosztów dodatkowych związanych z realizacją przedmiotu umowy. Nieuwzględnienie przez Wykonawcę jakichkolwiek kosztów na etapie przygotowania oferty nie może być podstawą jakichkolwiek roszczeń Wykonawcy w stosunku do Zamawiającego.

2. Zapłata przez Zamawiającego wynagrodzenia Wykonawcy nastąpi po odbiorze końcowym przedmiotu umowy przez Zamawiającego, na podstawie prawidłowo wystawionej faktury VAT.

3. Podstawą do wystawienia przez Wykonawcę faktury VAT będzie protokół końcowy podpisany przez Zamawiającego z klauzulą „bez zastrzeżeń” zgodnie z § 2 ust. 2 umowy, potwierdzający prawidłowe wykonanie przedmiotu umowy.

4. Zamawiający zapłaci kwotę wynikającą z faktury w terminie 30 dni od daty od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury przelewem na rachunek Wykonawcy wskazany na fakturze VAT.

5. W przypadku niedopełnienia zobowiązań Wykonawcy w zakresie prawidłowości i kompletności wymaganych treścią umowy, wystawionych i doręczonych przez Wykonawcę dokumentów, Zamawiający wstrzyma się od zapłaty należności z faktury do czasu uzupełnienia dokumentów lub ich korekty, przy czym termin zapłaty liczyć się będzie od dnia otrzymania przez Zamawiającego od Wykonawcy prawidłowych dokumentów.

6. Wykonawca oświadcza, że numer rachunku bankowego, który wskazany będzie na fakturze w celu dokonania na niego zapłaty przez Zamawiającego, figuruje na wykazie podmiotów („Biała lista”), o którym mowa w art. 96 b ust.1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.

7.Wykonawca zobowiązuje się nie dokonywać przelewu praw i obowiązków wynikających z niniejszej umowy jak również nie dokonywać ich przekazu oraz innych czynności podobnych zmierzających do zmiany podmiotowej uprawnień lub obowiązków po stronie Wykonawcy, wynikających z zawartej umowy pod rygorem nieważności.

**§ 4**

**Termin obowiązywania umowy**

Wykonawca wykona Przedmiot Umowy określony w § 1 umowy w terminie nie dłuższym niż do dnia ……….. (zgodnie z ofertą Wykonawcy).

**§ 5**

**Kary umowne**

1. Wykonawca ponosi odpowiedzialność za niewykonanie lub nienależyte wykonanie przedmiotu umowy.

2. Zamawiający może żądać od Wykonawcy kar umownych w następujących przypadkach:

1. 10 % wartości netto przedmiotu umowy, o której mowa w § 3 ust. 1 umowy, gdy Wykonawca odstąpi od umowy, z powodu okoliczności, za które odpowiada;
2. 10% wartości netto przedmiotu umowy, o której mowa w § 3 ust. 1 umowy, gdy Zamawiający odstąpi od umowy z powodu okoliczności leżących po stronie Wykonawcy;
3. 1% wartości netto przedmiotu umowy, o której mowa w § 3 ust. 1 umowy za każdy dzień zwłoki w realizacji przedmiotu umowy, licząc od terminu określonego w § 4;
4. 0,5% wartości netto przedmiotu umowy, o której mowa w §3 ust. 1 umowy, za każdy dzień zwłoki w przystąpieniu do usunięciu awarii/usterki/wady przedmiotu zamówienia, licząc od terminu określonego w § 2 ust. 5 umowy i w Opisie Przedmiotu zamówienia stanowiącym Załącznik nr 2 do Umowy;
5. 0,5 % wartości netto przedmiotu umowy, o której mowa w §3 ust. 1 umowy za każdy dzień zwłoki w usuwaniu usterek i wad sprzętu, licząc od terminów określonych w § 2 ust. 6 umowy.
6. braku realizacji w terminie obowiązku, o którym mowa w § 6 ust. 12 umowy – do wysokości 1 % wartości netto przedmiotu umowy, której brak realizacji dotyczy,
7. 0,5% wartości netto przedmiotu umowy, o której mowa w §3 ust. 1 umowy, za każdy dzień zwłoki w realizacji w terminie obowiązku, o którym mowa w § 6 ust. 12 umowy.

3. W przypadku gdy Wykonawca dostarczy i uruchomi rzecz zastępczą o tych samych funkcjonalnościach w miejsce rzeczy uszkodzonej kara umowna nie jest naliczana przez okres opóźnienia kiedy Zamawiający mógł korzystać z rzeczy zastępczej. Wykonawca może z tym samym skutkiem dostarczyć i uruchomić inną rzecz zastępczą o podobnych funkcjonalnościach po uzyskaniu zgody Zamawiającego.

4. Jeżeli kara umowna nie pokryje szkody strony, może ona dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

5. Wykonawca zobowiązuje się wyrównać w całości szkodę poniesioną przez Zamawiającego w przypadku utraty dotacji z powodu zwłoki w wykonaniu umowy, poprzez zapłatę odszkodowania równego wysokości utraconej dotacji.

6. Zamawiający może dochodzić na zasadach ogólnych odszkodowania przewyższającego kary umowne za nienależyte wykonywanie postanowień niniejszej umowy jak również za odstąpienie od umowy z przyczyn za które Wykonawca ponosi odpowiedzialność lub wyrównania wskazanego w ust. 6 powyżej.

7. Maksymalna wysokość kar umownych, których mogą dochodzić strony, z wszelkich tytułów przewidzianych w Umowie nie może przekraczać 50 % wynagrodzenia netto, o którym mowa w §3 ust. 1 umowy.

**§ 6**

**Gwarancja, rękojmia i warunki serwisu**

1. Wykonawca zobowiązuje się świadczenia nieodpłatnej usługi monitoringu infrastruktury IT do dnia …………. *(zgodnie z oferta Wykonawcy)*

2. Strony zgodnie postanawiają, że w okresie gwarancji określonym w Załączniku nr 2 do Umowy Wykonawca zobowiązuje się do bezpłatnego usuwania wad i usterek dostarczonego sprzętu lub bezpłatnej wymiany sprzętu na nowy, wolny od wad, w tym do załatwienia (na swój koszt i we własnym zakresie) wszelkich formalności związanych z: usunięciem wad, wysyłką do naprawy gwarancyjnej i odbiorem z naprawy, wymianą sprzętu na nowy, a także gdy zajdzie taka potrzeba w tym okresie wymienić części eksploatacyjne.

3. W przypadku stwierdzenia wad jakościowych sprzętu w okresie gwarancji Zamawiający złoży reklamację pisemnie e-mailem na następujący adres e-mail Wykonawcy…………………

4. Czas reakcji serwisu (rozumiany jako kontakt telefoniczny lub rozpoczęcie interwencji zdalne) od przyjęcia zgłoszenia awarii mailem na adres podany w umowie w czasie do 48 godz.

5. Czas usunięcie awarii, usterki lub wady (rozumiane jako przywrócenie pierwotnej funkcjonalności) od powzięcia wiadomości o zaistniałych wadach do 5 dni roboczych.

6. Termin, o którym mowa w ust. 5 powyżej może ulec wydłużeniu za zgodą Zamawiającego z przyczyn niezależnych od Wykonawcy, a wynikających z wymogów natury technicznej, procesu technologicznego lub innych wymogów o obiektywnym charakterze, o czym Wykonawca zobowiązany jest poinformować pisemnie Zamawiającego. W takim przypadku czas usuwania wad/usterek/awarii nie może być dłuższy niż 5 dni od dnia przekazania/udostępnienia przez Zamawiającego sprzętu do naprawy.

7. Termin gwarancji biegnie na nowo dla elementów sprzętu podlegającego wymianie, a w przypadku usuwania wad/ usterek/awarii ulega przedłużeniu o czas ich usunięcia (tj. o czas wyłączenia sprzętu z eksploatacji z powyższego powodu).

8. Jeżeli wady nie da się usunąć (sprzętu nie da się naprawić) Wykonawca jest zobowiązany niezwłocznie dostarczyć Zamawiającemu nowy sprzęt posiadający takie same parametry jak sprzęt, którego wady nie da się usunąć.

9. W przypadku 3-krotnej naprawy (w czasie obowiązywania gwarancji) tego samego elementu Wykonawca jest zobowiązany niezwłocznie wymienić sprzęt na nowy posiadający takie same parametry jak sprzęt, którego dotyczyła naprawa.

10. W przypadku rozbieżności w zapisach pomiędzy kartą gwarancyjną wydaną Zamawiającemu, a zapisami niniejszej umowy, pierwszeństwo zastosowania mają postanowienia niniejszej umowy

11. Niezależnie od uprawnień z gwarancji Zamawiającemu przysługują uprawnienia z tytułu rękojmi, na zasadach określonych w Kodeksie cywilnym. Okres rękojmi odpowiada okresowi udzielonej gwarancji i liczony będzie od daty odbioru sprzętu przez Zamawiającego, potwierdzonego protokołem zdawczo-odbiorczym z klauzulą „bez zastrzeżeń”, o którym mowa w § 2 ust. 1 umowy.

12. Wykonawca gwarantuje wykonywanie w okresie gwarancji w ramach wynagrodzenia przeglądów technicznych zgodnie z zaleceniem producenta, w tym w zakreślonych przez producenta terminach. Dotrzymanie terminów przeglądów leży po stronie Wykonawcy bez wcześniejszego wzywania do ich wykonania przez Zamawiającego. W ramach przeglądów technicznych Wykonawca zapewnia na swój koszt aktualizację oprogramowania do najnowszej wersji. Po wykonaniu wymaganych przeglądów technicznych Wykonawca zobowiązany jest do sporządzenia i przedłożenia Zamawiającemu raportów serwisowych.

13. Zamawiający zastrzega sobie prawo skorzystania na koszt i ryzyko Wykonawcy z usług zastępczych w przypadku nie wywiązania się Wykonawcy ze zobowiązań gwarancyjnych lub zobowiązań z tytułu rękojmi za wady, po uprzednim wezwaniu Wykonawcy do wykonania tych zobowiązań z wyznaczeniem dodatkowego terminu, co nie wyłącza prawa Zamawiającego do naliczenia kar umownych.

14. W przypadku, gdy przedmiot umowy lub jego część objęta jest gwarancją producenta (którym jest podmiot inny niż Wykonawca) Wykonawca obowiązany jest wydać Zamawiającemu karty gwarancyjne producenta/ich kopie oraz wszystkie dostępne i niezbędne dokumenty umożliwiające realizację uprawnień z gwarancji udzielonej przez producenta.

15. Wykonawca zobowiązany jest działać w sposób umożliwiający uzyskanie i zachowanie gwarancji producenta przez Zamawiającego.

**§ 7**

**Rozwiązanie umowy**

1. Poza przypadkami określonymi w kodeksie cywilnym Zamawiający może odstąpić od umowy lub jej części w przypadku niewykonania lub nienależytego wykonania przez Wykonawcę obowiązków wynikających z niniejszej umowy, a w szczególności w przypadku:

1. gdy Wykonawca opóźnia się w zakończeniu realizacji przedmiotu umowy powyżej 30 dni w stosunku do terminu określonego w § 4 ust. 1 umowy,
2. nieusunięcia przez Wykonawcę stwierdzonych w trakcie odbioru wad, niezgodności z umową (zawartych w protokole usterek),
3. braku realizacji przedmiotu umowy w terminie, o którym mowa w § 4 ust. 1 umowy i naliczenia kary umownej określonej w sytuacjach przewidzianych w § 5 umowy.

2. W przypadku odstąpienia od umowy z przyczyn określonych w ust. 1 Zamawiający nie traci uprawnienia do naliczenia kar umownych należnych Zamawiającemu na podstawie § 5 umowy.

3. Zamawiającemu przysługuje prawo odstąpienia od umowy lub jej części w każdym przypadku niewykonania lub nienależytego wykonania umowy przez Wykonawcę oraz w przypadkach opisanych w umowie, w terminie 30 dni od powzięcia wiadomości o okolicznościach stanowiących podstawę odstąpienia od umowy.

4. Zamawiający informuje Wykonawcę, iż niezależnie od postanowień umowy uprawniony jest do odstąpienia od umowy w sytuacji i na warunkach określonych w art. 456 ust. 1, pkt. 2) ustawy prawo zamówień publicznych.

5. W przypadku, o którym mowa w ust. 1 i 3 powyżej Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu prawidłowego i terminowego wykonania części umowy do momentu odstąpienia od niej przez Zamawiającego.

6. Czynność odstąpienia od umowy winna nastąpić w formie pisemnej po uprzednim, pisemnym wezwaniu Wykonawcy do należytego wykonania przedmiotu Umowy.

**§ 8**

**Wybór Sądu**

1. Ewentualne kwestie sporne wynikłe w trakcie realizacji niniejszej umowy strony rozstrzygać będą w pierwszym rzędzie polubownie.

2. W przypadku nie dojścia do porozumienia w terminie 30 dni od dnia doręczenia drugiej stronie wezwania do usunięcia naruszeń umowy lub też spełnienia zobowiązań umownych, spory rozstrzygane będą przez Sąd powszechny właściwy dla siedziby Zamawiającego.

3. W sprawach nie unormowanych niniejszą Umową zastosowanie mają przepisy Kodeksu Cywilnego (t.j. Dz. U. z 2020 r. poz. 1740 z późn. zm.) i ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129 z późn. zm.).

**§ 9**

**Zmiany zawartej umowy**

1. Zamawiający dopuszcza zmianę postanowień umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w razie wystąpienia następujących okoliczności, z uwzględnieniem podanych warunków ich wprowadzenia:

1. zmiany numeru rachunku bankowego, nazwy i innych danych Stron umowy, w przypadku zmiany tych danych,
2. zmiany oferowanego sprzętu na sprzęt o parametrach nie gorszych niż oferowany w przypadku wycofania oferowanego sprzętu z rynku, wstrzymania produkcji, w cenie nie wyższej niż oferowana,
3. zmiany stawki podatku VAT – przez odpowiednią zmianę wynagrodzenia brutto Wykonawcy. Strony są zobowiązane do niezwłocznego zawarcia odpowiedniego aneksu w przypadku wystąpienia zmiany stawki podatku VAT,
4. zmiany przepisów prawa, których wejście w życie lub zmiana nastąpiły po zawarciu umowy, a które mają wpływ na realizację umowy i z których wynika konieczność lub zasadność wprowadzenia zmian postanowień umowy (dostosowania treści umowy do aktualnego stanu prawnego),
5. wydłużenia terminu realizacji, o którym mowa w § 4 ust. 1 umowy z przyczyn organizacyjnych leżących po stronie Zamawiającego.

2. Zmiany określone w punkcie poprzedzającym nie mogą być niekorzystne dla Zamawiającego, w szczególności nie mogą skutkować niekorzystną dla niego zmianą wartości umowy, z wyłączeniem pkt c) ust. 1 powyżej.

3. Wniosek o dokonanie zmiany umowy należy przedłożyć na piśmie, a okoliczności mogące stanowić podstawę zmiany umowy powinny być uzasadnione i w miarę możliwości również udokumentowane przez Wykonawcę.

4. Zmiana umowy wymaga zgody obydwu stron.

5. Zmiany są dopuszczalne, jeżeli zachodzi co najmniej jedna z następujących okoliczności:

1. zmiany zostały przewidziane w ogłoszeniu o zamówieniu lub specyfikacji warunków zamówienia w postaci jednoznacznych postanowień umownych, które określają ich zakres, w szczególności możliwość zmiany wysokości wynagrodzenia wykonawcy, i charakter oraz warunki wprowadzenia zmian;
2. zmiany dotyczą realizacji dodatkowych dostaw, usług lub robót budowlanych od dotychczasowego Wykonawcy, nieobjętych zamówieniem podstawowym, o ile stały się niezbędne i zostały spełnione łącznie następujące warunki:
3. zmiana Wykonawcy nie może zostać dokonana z powodów ekonomicznych lub technicznych, w szczególności dotyczących zamienności lub interoperacyjności sprzętu, usług lub instalacji, zamówionych w ramach zamówienia podstawowego,
4. zmiana Wykonawcy spowodowałaby istotną niedogodność lub znaczne zwiększenie kosztów dla zamawiającego,
5. wartość każdej kolejnej zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie lub umowie ramowej;
6. zostały spełnione łącznie następujące warunki:
7. konieczność zmiany umowy lub umowy ramowej spowodowana jest okolicznościami, których Zamawiający, działając z należytą starannością, nie mógł przewidzieć,
8. wartość zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie lub umowie ramowej;
9. Wykonawcę, któremu Zamawiający udzielił zamówienia, ma zastąpić nowy Wykonawca:
10. na podstawie postanowień umownych, o których mowa w pkt 1 powyżej,
11. w wyniku połączenia, podziału, przekształcenia, upadłości, restrukturyzacji lub nabycia dotychczasowego wykonawcy lub jego przedsiębiorstwa, o ile nowy wykonawca spełnia warunki udziału w postępowaniu, nie zachodzą wobec niego podstawy wykluczenia oraz nie pociąga to za sobą innych istotnych zmian umowy,
12. w wyniku przejęcia przez zamawiającego zobowiązań wykonawcy względem jego podwykonawców;
13. zmiany, niezależnie od ich wartości, nie są istotne w rozumieniu art. 454 ust. 2 ustawy Pzp;
14. łączna wartość zmian jest mniejsza od 10% wartości zamówienia określonej pierwotnie w umowie w przypadku zamówień na dostawy.

6. Postanowienia umowne zmienione z naruszeniem ust. 5 powyżej podlega unieważnieniu. Na miejsce unieważnionych postanowień umowy wchodzą postanowienia umowne w pierwotnym brzmieniu.

**§ 10**

**Obowiązki zachowania poufności**

1. Zobowiązanie do zachowania poufności co do informacji pozyskanych w związku z realizacją niniejszej umowy obowiązuje przez okres trwania umowy i 10 lat po jej zakończeniu.

2. Zgodnie z art. 96 ust. 1 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych Wykonawca ma obowiązek zachowania poufności na zasadach przewidzianych w niniejszej umowie, a także zapewnienia, by wszelkie informacje poufne, jakie Wykonawca uzyska w toku realizacji umowy, a przekazane przez Zamawiającego lub pozyskane przez pracowników Wykonawcy, jego podwykonawców lub osoby współpracujące z Wykonawcą przy realizacji umowy na jakiejkolwiek podstawie prawnej, jak i bez tej podstawy, były zachowane w poufności na zasadach co najmniej takich, jak zasady obowiązujące Wykonawcę. Wykonawca/podwykonawca nie może wykorzystywać pozyskanych danych w żaden inny sposób lub w inny celu niż dla wykonywania niniejszej Umowy.

3. Wykonawca zobowiązany jest do przedłożenia Zamawiającemu w terminie 7 dni od daty zawarcia umowy, imiennego wykazu osób, które mają dostęp do informacji poufnych wraz z określeniem podstawy ich zatrudnienia lub współpracy z Wykonawcą (co najmniej rodzaj umowy, zakres czynności, okres obowiązywania).

4. Wraz z wykazem, o którym mowa w ust. 3 powyżej powyżej Wykonawca zobowiązany jest przedłożyć Zamawiającemu oryginały oświadczeń osób wskazanych w wykazie, obejmujące zobowiązanie tych osób do zachowania poufności na zasadach przewidzianych w niniejszym paragrafie dla Wykonawcy zawierające co najmniej:

1. dokładne oznaczenie podmiotu lub osoby składającej oświadczenie,
2. treść oświadczenia o zobowiązaniu do zachowania poufności wraz z określeniem okresu obowiązywania tego zobowiązania,
3. datę i miejsce złożenia oświadczenia,
4. podpis osoby składającej oświadczenie lub osoby uprawnionej do reprezentacji podmiotu.

5. Powyższy obowiązek dotyczy również wszystkich Podwykonawców uczestniczących w realizacji przedmiotu zamówienia.

**§ 12**

* + - * 1. **Osoby do kontaktu w sprawie realizacji umowy**

1. Wszelkie zawiadomienia i oświadczenia stron związane z niniejszą umową powinny być sporządzone w formie pisemnej na adres podany w komparycji umowy (chyba, że w umowie przewidziana została inna forma lub inny sposób doręczenia).

2. Korespondencja w toku realizacji niniejszej umowy – lecz nie zawiadomienia i oświadczenia przewidziane w jej treści (chyba, że wynika to wprost z treści umowy) – może odbywać się telefonicznie lub mailowo, na następujące adresy:

* 1. dla Zamawiającego: Pan/Pani …………………………,mail………………………………

tel. ……………………….,

* 1. dla Wykonawcy: Pan/Pani …………………………… , mail: …………………………...

tel. …………………………,

1. Każda ze Stron może zmienić swój adres do doręczeń w drodze pisemnego zawiadomienia wysłanego do drugiej Strony, przy czym zmiana adresu będzie skuteczna pod warunkiem otrzymania takiego zawiadomienia przez drugą Stronę i nie wymaga zmiany umowy.

**§ 13**

**Informacje dodatkowe**

1. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach.

2. Załączniki do Umowy stanowią integralną część Umowy.

Załącznik nr 1 - Oferta Wykonawcy

Załącznik nr 2 - Opis Przedmiotu Zamówienia.

**Zamawiający: Wykonawca:**

**Załącznik Nr 3b do SWZ**

**Umowa Nr /P/2022**

**na wykonanie audytu bezpieczeństwa systemów teleinformatycznych**

zawarta dnia …...……….….. w Puławach, pomiędzy:

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej z siedzibą w Puławach przy ul. Bema 1,   
24-100 Puławy, zarejestrowanym w rejestrze stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej prowadzonego przez Sąd Rejonowy Lublin - Wschód w Lublinie z siedzibą w Świdniku, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000026256, NIP 716-22-38-942, REGON 431205731

reprezentowanym przez:

- Piotra Rybaka – Dyrektora

zwanym dalej **„Zamawiającym”**

oraz

**………………………**. z siedzibą w ……………………………………………………… wpisanym do …………………………………………………………………………………….. prowadzonego przez Sąd Rejonowy dla ……………………., ……… Wydział Krajowego Rejestru Sądowego pod numerem KRS…………………….., NIP……………………….., REGON …………………...,

zwanym w dalszej części umowy **„Wykonawcą”** lub **„Stroną”**,

reprezentowanym przez:

…………………………………………..……..……….………………………………………...

zwani łączni w dalszej części umowy **„Stronami”**,

o następującej treści:

Zamawiający i Wykonawca będą dalej łącznie zwani „Stronami”, a każdy z nich z osobna także „Stroną”.

Wobec wyboru oferty Wykonawcy jako najkorzystniejszej w przeprowadzonym przez Zamawiającego postępowaniu w sprawie udzielenia zamówienia w trybie przetargu podstawowego  
nr ZM 45/230/2022 i na warunkach określonych w SWZ na podstawie ustawy z dnia 11 września 20019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.) (dalej: ustawa Pzp) Strony postanawiają co następuje:

**§ 1**

**Przedmiot Umowy**

1. Zamawiający zleca, zaś Wykonawca przyjmuje do wykonania przeprowadzenie i udokumentowanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego.

2. Szczegółowy opis przedmiotu Umowy znajduje się w Załączniku nr 2 do Umowy - „Opis przedmiotu zamówienia”.

**§ 2**

**Termin realizacji**

1. Wykonawca wykona Przedmiot Umowy określony w § 1 w terminie nie dłuższym niż do dnia …………………….. *(zgodnie z ofertą Wykonawcy),* w tym:

1) Spotkanie koordynacyjne Stron i szczegółowe zaplanowanie realizacji usługi - do 7 dni roboczych od dnia zawarcia Umowy,

2) Wnikliwa analiza poziomu bezpieczeństwa teleinformatycznego Zamawiającego ze stanu początkowego z uwzględnieniem Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa.

3) Przeprowadzenie Audytu poziomu bezpieczeństwa teleinformatycznego u Zamawiającego po wdrożeniu przez Zamawiającego czynności podnoszących poziom bezpieczeństwa systemów teleinformatycznych - do ……. dni roboczych od dnia powiadomienia przez Zamawiającego Wykonawcy o gotowości do poddania się Audytowi.

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

2. Termin wykonania Przedmiotu Umowy określony w § 2 ust 1. ulega odpowiedniemu przesunięciu o czas trwania opóźnień, które wynikły z winy Zamawiającego.

**§ 3**

**Wynagrodzenie**

1. Za pełne i prawidłowe wykonanie przedmiotu Umowy Wykonawca otrzyma wynagrodzenie w kwocie ………….. zł **netto** (słownie: …………………………..) plus należny podatek VAT, co stanowi kwotę **brutto** ………………. (słownie: …………………………..).
2. Wynagrodzenie Wykonawcy jest ostateczne i obejmuje wszystkie koszty, jakie mogą powstać w związku z realizacją przedmiotu Umowy, w tym wszelkie opłaty i podatki, wynagrodzenie z tytułu przeniesienia autorskich praw majątkowych oraz zależnych praw autorskich, o których mowa w §9, do utworów wykonanych w ramach Umowy, na polach eksploatacji wskazanych w §9 ust. 2 oraz wynagrodzenie z tytułu przeniesienia własności egzemplarzy utworów oraz ich nośników.
3. Podstawą do wystawienia przez Wykonawcę faktury będzie Protokół odbioru podpisany przez Zamawiającego bez zastrzeżeń.
4. Wynagrodzenie będzie płatne w terminie 30 dni od daty wpływu do Zamawiającego prawidłowo wystawionej faktury.
5. Wynagrodzenie będzie płatne przelewem na konto Wykonawcy wskazane na fakturze.
6. Za termin płatności przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego należną Wykonawcy kwotą.

**§ 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. Osoby wyznaczone do wykonania Umowy posiadają kwalifikacje, wiedzę i doświadczenie.

3. W trakcie obowiązywania Umowy Wykonawcy przysługiwać będzie prawo do zastępowania za zgodą Zamawiającego członków personelu Wykonawcy innymi osobami, o co najmniej takich samych odpowiednio kwalifikacjach lub doświadczeniu. Zamawiający dokona akceptacji zmiany osób wskazanych do realizacji Umowy w ciągu 3 dni od zgłoszenia jej przez Wykonawcę.

4. W przypadku zmiany osoby wskazanej na danym stanowisku, danej roli, osoba zastępująca musi posiadać odpowiednio doświadczenie zawodowe i/lub kwalifikacje nie gorsze niż osoba zastępowana.

5. Zasady opisane w ust. 3 i 4 będą miały zastosowanie również w przypadku wskazania przez Wykonawcę dodatkowych osób do skierowanych do realizacji zadań.

6. Zamawiający ma prawo zażądać zmiany członka personelu Wykonawcy w przypadku pojawienia się uzasadnionych zastrzeżeń, co do jego kwalifikacji, wiedzy, rzetelności lub terminowości wykonywania obowiązków. Zamawiający zobowiązany jest przekazać zastrzeżenia w formie pisemnej. W takim przypadku Wykonawca dokona zmiany członka personelu na nowego, nie później niż w terminie 5 dni od zgłoszenia zastrzeżeń przez Zamawiającego. Wykonawca zobowiązany jest poinformować Zamawiającego o zaprzestaniu wykonywania prac przez danego członka personelu Wykonawcy, w terminie 7 dni od nastąpienia tego zdarzenia. Każda zmiana personelu, o której mowa powyżej, skutkuje odbiorem lub nadaniem uprawnień do systemów przez Zamawiającego.

7. Zmiana osób, o której mowa powyżej, nie stanowi zmiany Umowy i nie wymaga zawarcia aneksu do Umowy. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o powyższej zmianie w formie pisemnej oraz zapewnienia transferu wiedzy pomiędzy osobami zastępowaną i zastępującą, jak również realizacji innych obowiązków wynikających z Umowy względem nowego członka personelu.

8. Osobami uprawnionymi do bieżących kontaktów w ramach realizacji przedmiotu umowy oraz do odbioru Raportu i podpisywania protokołów są osoby:

* 1. po stronie Zamawiającego: …………………………………...
  2. po stronie Wykonawcy: ……………………….………………..

**§ 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) umożliwienia Wykonawcy wykonania przedmiotu Umowy określonego w § 1 ust. 1 Umowy.

2. Strony zgodnie ustalają, iż 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, iż powyższymi adresami posługiwać się mogą wyłącznie osoby upoważnione do kontaktów z drugą Stroną.

3. Wykonawca gwarantuje, że jego usługi będą świadczone w profesjonalny sposób, według odpowiedniej wiedzy i doświadczenia, z najwyższą starannością wymaganą od czołowych przedsiębiorstw IT w Polsce i efektywnością, oraz że wykona zlecone mu prace terminowo i zgodnie i obowiązującym stanem prawnym.

4. Wykonawca uprawniony będzie do realizacji przedmiotu Umowy w siedzibie Zamawiającego lub zdalnie po uzyskaniu pisemnej zgody Zamawiającego.

5. Wykonawca dołoży wszelkich starań w celu uniknięcia wpływu testów na prace testowanych systemów. Termin i zakres prowadzenia prac będzie każdorazowo uzgadniany z Zamawiającym, tak aby zminimalizować potencjalne skutki testów.

6. Wykonawca ponosi całkowitą odpowiedzialność za swoje działania lub zaniechania związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy Zamawiającego lub osoby trzeciej za którą Wykonawca nie ponosi odpowiedzialności.

7. Wykonawca nie jest uprawniony do wprowadzania jakichkolwiek zmian do systemów teleinformatycznych Zamawiającego bez pisemnej zgody Zamawiającego, w szczególności Wykonawca zobowiązuje się nie wprowadzać żadnych zmian do baz danych wykorzystywanych przez Zamawiającego.

**§ 6**

**Odbiór prac**

1. Wykonawca przekazuje Zamawiającemu Raport w terminie wskazanym w § 2 ust. 1 pkt 4.

2. O ile Zamawiający uzna, że Raport powinien mieć klauzulę „zastrzeżone”, Zamawiający nada ją według swojego uznania, o czym poinformuje Wykonawcę na adres określony w § 4 ust. 8 pkt 2.

3. Zamawiający w terminie do 5 dni roboczych zaakceptuje przekazany Raport albo zgłosi do niego uwagi, przesyłając je na adres określony w § 4 ust. 8 pkt 2.

4. W przypadku zgłoszenia uwag do Raportu 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 poprawiony Raport, nie późnej niż w terminie 5 dni roboczych od otrzymania uwag od Zamawiającego.

5. W przypadku zgłoszenia przez Zamawiającego dalszych uwag do wykonania przedmiotu Umowy, postanowienia ust. 3 i 4 stosuje się odpowiednio.

6. Odbiór Raportu nastąpi w formie Protokołu odbioru, podpisanego przez Zamawiającego bez zastrzeżeń.

7. Za termin wykonania przedmiotu umowy strony uznają dzień podpisania przez Zamawiającego protokołu odbioru bez zastrzeżeń.

**§ 7**

**Kary umowne**

1. Wykonawca jest zobowiązany do zapłaty kar umownych:

1) w przypadku odstąpienia od umowy przez Wykonawcę lub przez Zamawiającego z przyczyn leżących po stronie Wykonawcy - w wysokości 30% wynagrodzenia brutto, o którym mowa w § 3 ust. 1,

2) w przypadku zwłoki w wykonaniu umowy ponad termin określony w § 2 ust. 1 - w wysokości 5 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 za każdy dzień zwłoki z zastrzeżeniem § 2 ust. 2 Umowy.

3) za każdy stwierdzony przypadek ujawnienia jakiejkolwiek informacji lub innego naruszenia bezpieczeństwa informacji, w okresie obowiązywania umowy, jak też i po jej wygaśnięciu lub rozwiązaniu, w tym niewykonanie obowiązku określonego w § 11 ust. 12 - w wysokości 20% wynagrodzenia brutto, o którym mowa w § 3 ust. 1.

2. W przypadku niedokonania przez Wykonawcę na żądanie Zamawiającego zmiany członka personelu, zgodnie z warunkami określonymi w § 4, w terminie 5 dni od dnia zgłoszenia zastrzeżeń przez Zamawiającego, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1500 zł za każdy dzień zwłoki w wykonaniu powyższego obowiązku.

3. W przypadku realizacji Umowy 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, Wykonawca zapłaci Zamawiającemu karę w wysokości 1500 zł za każdy dzień świadczenia usługi przez Wykonawcę z udziałem ww. osoby.

4. Kary umowne mogą podlegać sumowaniu oraz mogą być naliczane niezależnie od siebie z tym zastrzeżeniem, że jeśli to samo działanie lub zaniechanie Wykonawcy wypełnia przesłanki do naliczenia dwóch lub więcej kar umownych wskazanych w Umowie, to Zamawiający naliczy karę wyższą, nie może on jednak nałożyć więcej niż jednej kary za to samo działanie czy zaniechanie. Kary będą naliczane za każdy przypadek naruszenia Umowy odrębnie.

5. W przypadku zaistnienia przesłanek naliczenia kary umownej, Zamawiający wystawi notę obciążeniową z terminem płatności nie krótszym niż 7 dni.

6. Jeżeli szkoda przewyższy wysokość kary umownej, Zamawiającemu przysługiwać będzie roszczenie o zapłatę odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.

7. Wykonawca ponosi odpowiedzialność za szkody wyrządzone Zamawiającemu przy wykonywaniu lub w związku z wykonywaniem postanowień umowy. Kary umowne wskazane powyżej przysługują Zamawiającemu także w przypadku odstąpienia od umowy lub jej wypowiedzenia, niezależnie od kary umownej z tytułu odstąpienia lub wypowiedzenia umowy.

8. Łączna wysokość kar umownych ograniczona jest do 50 % 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 nie kontynuuje jej niezwłocznie po wezwaniu złożonym na piśmie przez Zamawiającego.

2. Zamawiającemu przysługuje prawo do wypowiedzenia umowy w trybie natychmiastowym, bez zachowania okresu wypowiedzenia w następujących przypadkach:

1) w przypadku niewykonania lub nienależytego wykonywania przedmiotu umowy przez Wykonawcę – w takim wypadku Zamawiający wyznaczy Wykonawcy dodatkowy 5-dniowy termin na wykonanie zobowiązania. Jeśli Wykonawca nie rozpocznie w ww. terminie wykonywania przedmiotu umowy w sposób należyty, Zamawiający ma prawo wypowiedzieć umowę ze skutkiem na dzień złożenia wypowiedzenia,

2) naruszył bezpieczeństwo informacji lub zasady z nim związane.

3. W przypadku zwłoki w realizacji przedmiotu Umowy przekraczającej 7 dni ponad termin wskazany w §2 ust. 1 Zamawiający może, niezależnie od nałożenia na Wykonawcę kar umownych, odstąpić od umowy w całości lub w części. Termin ten ulega odpowiedniemu przesunięciu o czas trwania opóźnień, które wynikły z winy Zamawiającego

4. Oświadczenie o odstąpieniu lub wypowiedzeniu powinno być złożone na piśmie i zostać dostarczone drugiej Stronie.

5. Zamawiający może odstąpić od Umowy w terminie 30 dni od daty zaistnienia zdarzenia stanowiącego podstawę do odstąpienia.

6. Odstąpienie od umowy nie wpływa na obowiązek zachowania poufności informacji.

7. W razie odstąpienia od umowy lub jej wypowiedzenia, Zamawiający – w ramach należnego Wykonawcy wynagrodzenia - nabywa autorskie prawa majątkowe i zależne prawa autorskich do utworów oraz utworów i ich nośników, odnośnie do których Zamawiający praw nie nabył, w zakresie określonym w § 9, z chwilą złożenia oświadczenia o odstąpieniu lub wypowiedzeniu.

8. Siła wyższa:

1) Żadna Strona nie będzie odpowiedzialna za niewykonanie swoich zobowiązań w ramach umowy w stopniu, w jakim opóźnienie w jej działaniu lub inne niewykonanie jej zobowiązań jest wynikiem Siły Wyższej.

2) Dla potrzeb umowy „Siła Wyższa” oznacza wydarzenie nadzwyczajne pozostające poza kontrolą Strony, występujące po podpisaniu umowy przez obie Strony, przeszkadzające racjonalnemu wykonaniu przez tę Stronę jej obowiązków, nie obejmujące winy własnej lub nienależytej staranności tej Strony i nieprzewidywalne w dacie zawarcia umowy.

3) Jeżeli Siła Wyższa spowoduje niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy:

a) Strona – o ile będzie to możliwe - zawiadomi w terminie 2 dni na piśmie drugą Stronę o powstaniu i zakończeniu tego zdarzenia, w miarę możliwości przedstawiając stosowną dokumentację w tym zakresie,

b) Strona niezwłocznie przystąpi do dalszego wykonywania umowy,

c) Strony uzgodnią sposób postępowania wobec tego zdarzenia oraz terminy wykonywania umowy.

9. Jeżeli Siła Wyższa spowoduje niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy przez okres powyżej trzech (3) tygodni, Strony spotkają się i w dobrej wierze rozpatrzą celowość i warunki rozwiązania umowy.

**§ 9**

**Prawa autorskie**

1. Wykonawca oświadcza, że będą mu przysługiwały autorskie prawa majątkowe i prawa zależne do wszelkich utworów, które powstaną w wyniku wykonania Umowy.

2. Wykonawca, z dniem podpisania protokołu odbioru Raportu, przenosi na Zamawiającego autorskie prawa majątkowe do Raportu , na następujących polach eksploatacji:

1) w zakresie utrwalania i zwielokrotniania Raportu, - wytwarzanie określoną techniką egzemplarzy, w tym drukarską reprograficzną, elektroniczną, fotograficzną, cyfrową, audiowizualną, technikami multimedialnymi oraz zapisu magnetycznego obejmujące trwałe lub czasowe utrwalanie lub zwielokrotnianie w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu bez ograniczeń co do ilości egzemplarzy oraz korzystania i rozporządzania tymi egzemplarzami;

2) w zakresie obrotu oryginałem albo egzemplarzami, na których Raportu utrwalono - wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;

3) w zakresie rozpowszechniania Raportu, w sposób inny niż określony w pkt 2 - publiczne wykonanie, wyświetlenie, odtworzenie, nadanie i reemitowanie, a także publiczne udostępnienie Raportu, w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym.

3. Wykonawca przenosi na rzecz Zamawiającego, w ramach wynagrodzenia przewidzianego niniejszą umową, z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, prawo zezwalania na wykonanie zależnego prawa autorskiego, w tym do rozporządzania i korzystania z opracowań Raportu, w nieograniczonym zakresie, w szczególności w zakresie pól eksploatacyjnych wskazanych w ust. 2.

4. Z chwilą podpisania przez Zamawiającego protokołu odbioru Raportu, Zamawiający nabywa na własność egzemplarze Raportu, przekazane przez Wykonawcę oraz nośniki, na których Raport utrwalono.

5. Zamawiający nie ponosi odpowiedzialności za naruszenie autorskich praw majątkowych lub osobistych wobec osób trzecich. Wykonawca zobowiązuje się do nieodwołalnego i bezwarunkowego zwolnienia Zamawiającego, na pierwsze żądanie, z wszelkich roszczeń, wynikających z naruszenia majątkowych i osobistych praw autorskich, do którego doszło z przyczyn leżących po stronie Wykonawcy.

6. Wykonawca oświadcza, że przygotowany przez niego Raport będzie oryginalny i nie będzie naruszał praw osób trzecich oraz będzie wolny od wad. Wykonawca zobowiązuje się, że w momencie przekazywania Raportu Zamawiającemu będzie wyłącznym ich dysponentem majątkowym praw autorskich.

7. Przeniesienie autorskich praw majątkowych zostaje dokonane na czas nieokreślony i jest nieograniczone terytorialnie.

8. W przypadku ujawnienia nowego pola eksploatacji mającego znaczenie dla Zamawiającego, Strony ustalają, że Wykonawca na wezwanie Zamawiającego przeniesie na Zamawiającego, w terminie 14 dni od doręczenia Wykonawcy wezwania, autorskie prawa majątkowego do Raportu oraz prawo zezwalania na wykonywanie praw zależnych do Raportu na nowym polu eksploatacji, na zasadach określonych w niniejszej umowie. Przeniesienie praw, o których mowa w zdaniu poprzednim, zostanie dokonane na rzecz Zamawiającego w ramach wynagrodzenia przewidzianego niniejszą umową.

**§ 10**

**Rozstrzyganie sporów**

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

**§ 11**

**Ochrona informacji**

1. Informacją w rozumieniu Umowy są wszelkie informacje, dokumenty lub dane przekazane Wykonawcy przez Zamawiającego, uzyskane przez Wykonawcę w związku z realizacją Umowy oraz wytworzone przez Wykonawcę na potrzeby realizacji Umowy.

2. Wykonawca może przetwarzać powierzone mu przez Zamawiającego informacje przez okres obowiązywania Umowy.

3. Wykonawca zobowiązuje się po zakończeniu realizacji Umowy do zwrotu Zamawiającemu wszelkich udostępnionych oraz wytworzonych przez siebie w związku z realizacją Umowy informacji, wraz z nośnikami. W przypadku utrwalenia na nośnikach należących do Wykonawcy informacji uzyskanych w związku z realizacją Umowy, Wykonawca zobowiązuje się do usunięcia z nośników tych informacji, w tym również sporządzonych kopii zapasowych, oraz zniszczenia wszelkich danych, dokumentów mogących posłużyć do odtworzenia, w całości lub części, informacji.

4. Wykonawca zobowiązuje się do przestrzegania wytycznych Zamawiającego o ochronie udostępnianych informacji.

5. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji, a także sposobów zabezpieczenia informacji, zarówno w trakcie trwania niniejszej Umowy, jak i po jej wygaśnięciu lub rozwiązaniu. Wykonawca ponosi pełną odpowiedzialność za zachowanie w tajemnicy ww. informacji przez osoby realizujące Umowę.

6. Wykonawca zobowiązany jest do zastosowania wszelkich niezbędnych środków technicznych i organizacyjnych zapewniających ochronę przetwarzania informacji, a w szczególności powinien zabezpieczyć informacje przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem postanowień Umowy, zmianą, utratą, uszkodzeniem, zniszczeniem lub kradzieżą.

7. Wykonawca zobowiązuje się do dołożenia najwyższej staranności w celu zabezpieczenia informacji przed bezprawnym dostępem, rozpowszechnianiem lub przekazaniem osobom trzecim.

8. Wykonawca zobowiązany jest zapewnić wykonanie obowiązków w zakresie bezpieczeństwa informacji, w szczególności dotyczącego zachowania w tajemnicy informacji, także przez jego pracowników oraz osoby, które realizują Umowę w imieniu Wykonawcy. Odpowiedzialność za naruszenie powyższego obowiązku spoczywa na Wykonawcy. Naruszenie bezpieczeństwa informacji, w szczególności ujawnienie jakiejkolwiek informacji w okresie obowiązywania Umowy, uprawnia do odstąpienia przez Zamawiającego od Umowy.

9. Wykonawca może udostępniać informacje jedynie tym swoim pracownikom lub osobom współpracującym na podstawie umów cywilnoprawnych, którym będą one niezbędne do wykonania powierzonych im czynności i tylko w zakresie, w jakim muszą mieć do nich dostęp dla celów określonych w niniejszej Umowie.

10. Wykonawca oraz inne osoby, które realizują Umowę w imieniu Wykonawcy, zobowiązane są przed przystąpieniem do prac do podpisania oświadczenia o zachowaniu poufności informacji. Podpisane oświadczenie należy przekazać Zamawiającemu przed rozpoczęciem realizacji Umowy przez ww. pracowników.

11. Wykonawca ponosi wszelką odpowiedzialność, tak wobec osób trzecich, jak i wobec Zamawiającego, za szkody powstałe w związku z nienależytą realizacją obowiązków dotyczących zapewnienia bezpieczeństwa informacji.

12. Wykonawca zobowiązuje się do ścisłego przestrzegania warunków niniejszej Umowy, które wiążą się z ochroną informacji, w szczególności nie może bez pisemnego upoważnienia Zamawiającego wykorzystywać informacji w celach niezwiązanych z realizacją Umowy.

13. W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji lub z naruszeniem obowiązków wynikających z Umowy, Zamawiający może przeprowadzić kontrolę wykonywanych przez Wykonawcę czynności. Kontrola może być realizowana przez Zamawiającego lub podmioty przez niego uprawnione. Wykonawca zobowiązany jest współpracować z Zamawiającym w odpowiednim zakresie z podmiotami przeprowadzającymi kontrolę. Wyniki kontroli zostaną przekazane Wykonawcy po jej zakończeniu. Zamawiający może wskazać niezbędne działania, jakie Wykonawca musi podjąć w celu wprowadzenia określonych zmian lub podjęcia określonych czynności.

14. Wykonawca zobowiązany jest do natychmiastowego powiadamiania o nieuprawnionym ujawnieniu lub udostępnieniu informacji oraz o innym naruszeniu bezpieczeństwa informacji, a następnie raportowania Zamawiającemu o podjętych działaniach w powyższym zakresie:

1) telefonicznie, na numer telefonu ……………………

2) na adres email: …………………

Powiadomienie dokonane telefonicznie musi zostać potwierdzone poprzez sposób wskazany w pkt 2) w terminie jednej godziny od dokonania powiadomienia.

15. Wykonawca nie może zwielokrotniać, rozpowszechniać, korzystać w celach niezwiązanych z realizacją Umowy oraz ujawniać informacji osobom trzecim, bez uzyskania w powyższym zakresie pisemnej zgody Zamawiającego, o ile takie informacje nie zostały już podane do publicznej wiadomości lub nie są publicznie dostępne.

16. Wykonawca zobowiązany jest:

1) zapewnić kontrolę nad tym, jakie informacje, kiedy, przez kogo oraz komu są przekazywane;

2) zapewnić, aby osoby, o których mowa w pkt 1, zachowywały w tajemnicy informacje oraz sposoby ich zabezpieczeń.

16. 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.

17. Wykonawca zobowiązany jest zapewnić bezpieczeństwo informacji przed wystąpieniem zagrożeń, w szczególności poprzez:

1) zastosowanie firewall oraz oprogramowania antyspamowego i antywirusowego,

2) zapewnienie kontroli dostępu do powierzonych zasobów Zamawiającego,

3) uniemożliwienie dostępu do haseł do zasobów informatycznych Zamawiającego przez osoby nieuprawnione wraz z ich cykliczną zmianą,

4) zastosowanie zabezpieczeń ochrony fizycznej.

**§ 12**

**Zmiany do Umowy**

1. O ile Umowa nie stanowi inaczej, zmiany treści Umowy mogą być dokonywane wyłącznie w formie aneksu podpisanego przez obie Strony, pod rygorem nieważności w zakresie:

1) zmiany szczegółowych zasad wykonywania przedmiotu Umowy określonych w załącznikach do Umowy, spowodowane zmianami organizacyjnymi u Zamawiającego;

2) zmiany zakresu realizacji Przedmiotu Umowy, w przypadku wystąpienia zmiany okoliczności powodującej, że:

a) realizacja części Przedmiotu Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawierania Umowy,

b) realizacja części Przedmiotu Umowy nie jest zasadna na skutek zmiany lub planowanej zmiany powszechnie obowiązujących przepisów prawa.

1) zmiany postanowień Umowy będące następstwem zmian powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy i z których treści wynika konieczność lub zasadność wprowadzenia zmian postanowień Umowy; powyższa zmiana dotyczy także zmiany postanowień Umowy w związku ze zmianą przepisów dotyczących ochrony danych osobowych, w szczególności w zakresie obowiązku spełniania przez Wykonawcę wymagań określonych przez Zamawiającego, poddania się kontroli oraz odstąpienia od Umowy przez Zamawiającego w związku z nieprzestrzeganiem przez Wykonawcę obowiązków związanych z ochroną danych osobowych lub poddaniu się kontroli;

2) zmiany terminu wykonania Umowy spowodowane zmianą powszechnie obowiązujących przepisów prawa, których wejście w życie lub zmiana nastąpiły po wszczęciu postępowania o udzielenie zamówienia publicznego, a które mają wpływ na realizację Umowy;

3) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest konieczna w celu prawidłowego wykonania Przedmiotu Umowy;

4) niezbędna jest zmiana terminu realizacji Umowy w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które obie Strony nie miały wpływu. W takim przypadku termin realizacji umowy zostanie odpowiednio wydłużony o czas trwania przyczyny uniemożliwiającej realizację Umowy;

2. Zmiany, o których mowa w ust. 1 pkt 1 - 6, nie mogą spowodować zwiększenia łącznego wynagrodzenia brutto, o którym mowa w § 3 ust. 1.

**§ 13**

**Postanowienia końcowe**

1. Wszelkie zmiany i uzupełnienia Umowy, jej wypowiedzenie, rozwiązanie za zgodą obu Stron lub odstąpienie od niej dokonywane będą w formie pisemnej pod rygorem nieważności.

2. Wykonawca bez zgody podmiotu tworzącego Zamawiającego nie może dokonać cesji wierzytelności.

3. Dla potrzeb Umowy Strony ustalają, że ilekroć w umowie jest mowa o dniach roboczych należy przez to rozumieć dni tygodnia przypadające od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

4. W trakcie wykonania przedmiotu Umowy Wykonawca będzie odpowiadać jak za swoje własne czyny za wszelkie czyny lub zaniechania swoich pracowników lub innych osób, którym Wykonawca powierzy za zgodą Zamawiającego wykonanie czynności związanych z realizacją Przedmiotu Umowy.

5. Niewykonanie przez Zamawiającego któregokolwiek z uprawnień przysługujących mu na podstawie Umowy nie może w żadnym razie być uważane za zrzeczenie się tego uprawnienia, ani zrzeczenie się innych uprawnień wynikających z postanowień Umowy.

6. Umowę sporządzono w 3 jednobrzmiących egzemplarzach: jeden dla Wykonawcy i dwa dla Zamawiającego.

7. Załączniki do Umowy stanowią integralną część Umowy.

Załącznik nr 1 – Oferta Wykonawcy

Załącznik nr 2 – Opis przedmiotu zamówienia

**Zamawiający: Wykonawca:**

**Załącznik nr 4 do SWZ**

**Zadanie nr 1**

# **Dostawa licencji systemów antywirusowych dla stacji roboczych i serwerów wraz z urządzeniem UTM. Dostawa Przełączników sieciowych wraz z systemem Zarządzania oraz systemem NAC. Opracowanie i wdrożenie wspólnych procedur bezpieczeństwa dla systemów sieciowych.**

W ramach wdrożenia spójnej polityki bezpieczeństwa reagowania na incydenty Zamawiający określa wymogi reagowania na incydenty bezpieczeństwa zgodnie z metodologią NIST:

- spójna polityka bezpieczeństwa dotycząca wszystkich systemów: systemy antywirusowe, systemy Firewall (IPS, IDS, UTM, Nework protection etc..) systemy kontroli sieci NAC, systemy backupu i replikacji oprogramowania.

-definiowanie planu reakcji na incydenty jako lista kroków do wykonania w momencie wystąpienia incydentu

- opracowanie procedur reagowania na incydenty – opracowanie szczegółowych kroków, które zespoły reagowania na incydenty będą wykorzystywać do reagowania na incydent. Powinny być one oparte na polityce i planie reagowania na incydenty i powinny obejmować wszystkie cztery fazy cyklu życia reakcji na incydenty: przygotowanie, wykrywanie i analizę, ograniczanie, eliminację i odzyskiwanie oraz działania po incydencie

Zamawiający wymaga aby Wykonawca stworzył spójne procedury bezpieczeństwa zgodnie z metodologią NIST uwzględniając systemy antywirusowe, systemy Firewall UTM oraz system kontroli dostępu NAC.

Zamawiający w szczególności wymaga aby w momencie wykrycia incydentu bezpieczeństwa system wykonał minimum następujące procedury:

1. Powiadomienie zespołu reagowania na incydenty o wykryciu incydentu

2. Odizolowanie stacji roboczej / Serwera lub innej maszyny działającej w sieci poprzez:

- Automatyczne wyłączenie na urządzeniu UTM wszystkich routingów z których korzystało dane urządzenie

- Przeniesienie do VLAN z którego nie ma dostępu do żadnej innej sieci Zamawiającego

3. Identyfikacja i diagnostyka incydentu

4. Procedura usunięcia i eliminacji zagrożenia incydentem oraz odtworzenia stanu sieci i urządzenia przed wystąpieniem incydentu bezpieczeństwa

5. Działania po wystąpieniu incydentu

## Wymagane parametry techniczne w zakresie dostarczanych licencji i sprzętu

|  |  |  |
| --- | --- | --- |
| **System antywirusowy** | | |
| 1. | Administracja zdalna | 1. Rozwiązanie Centralnej administracji musi wspierać instalację na systemach Windows Server, Linux lub być dostępne jako chmurowa usługa producenta 2. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 3. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami. 4. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, antyransomware które działają na stacjach roboczych w sieci. 5. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 6. Rozwiązanie musi zapewniać korzystanie z szablonów raportów, przygotowanych przez producenta. 7. Rozwiązanie musi zapewniać podział uprawnień administracyjnych. |
| 2. | Ochrona stacji roboczych | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. 3. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 4. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. 5. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. 6. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. 7. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów,. 8. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering. 9. Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy. |
| 3. | Ochrona Serwerów Windows | 1. Rozwiązanie musi wspierać systemy operacyjne Windows Server2016, Windows Server2019, Windows Server2022. 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. 3. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 4. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. 5. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. 6. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. 7. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów,. 8. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering. |
|  | Endpoint Detection and Response | 1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows, MacOS, Linux współpracujący z systemem do ochrony stacji roboczych i serwerów tego samego producenta. 2. Rozwiązanie musi mieć możliwość późniejszego rozszerzenia moduły EDR o logi pochodzące z platform Android, iOS tego samego producenta 3. Rozwiązanie musi pozwolić administratorom odszukać informację dotyczące incydentów związanych z bezpieczeństwem, zapewniając wgląd w zakres ataku, sposób jego rozpoczęcia, wpływ i sposób reagowania. 4. Rozwiązanie musi mieć opcję „ręcznego izolowania” chronionych punktów końcowych od sieci podczas badania przypadku zagrożenia. 5. Rozwiązanie musi zapewniać detekcję w oparciu o Mitre ATT&CK Tactic and Technique 6. Rozwiązanie musi pozwalać na wysyłanie powiadomień do administratora w chwili utworzenia nowego dochodzenia |
| UTM | Konstrukcja oraz porty | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.  Rozwiązanie powinno być wyposażone w moduł kryptoraficzny zgodny ze standardem FIPS 140-2.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)  Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active.  System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.  Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażęnie opcjonalne).  Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).  Wbudowany port Ethernet do zarządzania w trybie out-of-band management. |
| Utm | Wymagania Interface/przestrzeń | Przestrzeń do przechowywania logów i raportów nie mniej niż 12GB  Liczba fizycznych interfejsów 1000BASE-T nie mniej niż: 8  Liczba fizycznych interfejsów 1000BASE-X nie mniej niż: 2  Liczba fizycznych interfejsów 10GBASE-X nie mniej niż: 2  Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: 128 |
| Utm | Wydajność | Wydajność Firewall nie mniej niż (Gbps) 38  Wydajność Firewall IMIX nie mniej niż (Gbps) 22  Wydajność IPS nie mniej niż (Gbps) 9,8  Wydajność FW+IPS+AV nie mniej niż (Gbps) 2  Wydajność NGFW nie mniej niż (Gbps) 9  Liczba równoczesnych połączeń nie mniejsza niż: 12000000  Liczba nowych połączeń na sekundę nie mniejsza niż: 180000  Wydajność IPsec VPN nie mniej niż (Gbps): 17  Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps): 2,4  Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 55000  Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 5000  Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: 4000 |
| UTM | Uwierzytelnianie | Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.  System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.  System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).  Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. |
| UTM | Logowanie i Raportowanie | System musi możliwiać monitorowanie logów ruchu w czasie rzeczywistym.  System powinien umożliwiać składowanie oraz archiwizację logów.  Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.  Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.  System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.  System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. |
| UTM | IPS | Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.  Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.  Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.  System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. |

# **Przełącznik Dostępowy**

|  |  |  |
| --- | --- | --- |
| **Przełącznik Dostępowy** | | |
| 1. | Wymagania podstawowe | 1. Przełącznik posiadający    1. 48 portów 1G 10/100/1000BASE-T    2. 4 porty 1GBase-X SFP    3. 2 dedykowane porty do łączenia urządzeń w stos z przepustowością 40 Gbps    4. 1 dedykowany port Ethernet RJ45 do zarzadzania poza pasmem (out of band management    5. 1 dedykowany port konsoli szeregowej RJ45 2. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T 3. Wysokość urządzenia 1U 4. Przełącznik musi posiadać wbudowany zasilacz 230V AC. 5. Przełącznik musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza. 6. Nieblokującą architekturę o wydajności przełączania min. 175 Gb/s 7. Szybkość przełączania min. 130 Milionów pakietów na sekundę 8. Możliwość łączenia do 8 przełączników w stos 9. Musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych 10. Tablica MAC adresów min. 16k 11. Pamięć operacyjna: min. 1GB pamięci DRAM 12. Pamięć flash: min. 2GB pamięci Flash 13. Pojemność bufora pakietów min. 1,5 MB 14. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000 15. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci 16. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) 17. Obsługa Q-in-Q IEEE 802.1ad 18. Obsługa Quality of Service     1. IEEE 802.1p     2. DiffServ     3. 8 kolejek priorytetów na każdym porcie wyjściowym 19. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB 20. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) 21. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. 22. Wbudowany DHCP serwer i klient 23. Możliwość instalacji min. dwóch wersji oprogramowania - firmware 24. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash 25. Możliwość monitorowania zajętości CPU 26. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring) 27. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management. |
|  | Obsługa Routingu IPv4 | 1. Sprzętowa obsługa routingu IPv4 – forwarding 2. Pojemność tabeli routingu min. 450 wpisów 3. Routing statyczny 4. Obsługa routingu dynamicznego RIPv1/v2 5. Policy Based Routing dla IPv4 6. Obsługa DHCP/BootP Relay dla IPv4 |
|  | Obsługa Routingu IPv6 | 1. Sprzętowa obsługa routingu IPv6 – forwarding 2. Pojemność tabeli routingu min. 225 wpisów 3. Routing statyczny 4. Obsługa routingu dynamicznego dla RIPng 5. Obsługa MLDv1 (Multicast Listener Discovery version 1) 6. Obsługa MLDv2 (Multicast Listener Discovery version 2) 7. Policy Based Routing dla IPv6 8. Obsługa DHCP/BootP Relay dla IPv6 9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106 |
|  | Obsługa Multicastów | 1. Statyczne przyłączenie do grupy multicast 2. Filtrowanie IGMP 3. Obsługa Multicast VLAN Registration - MVR 4. Obsługa IGMP v1/v2/v3 5. Obsługa IGMP v1/v2/v3 snooping |
|  | Bezpieczeństwo | 1. Obsługa Network Login    1. IEEE 802.1x - RFC 3580    2. Web-based Network Login    3. MAC based Network Login 2. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants) 3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) 4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC 5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login 6. Urządzenie musi wspierać profile bezpieczeństwa, profil bezpieczeństwa oznacza połączenie:    1. definicji sieci VLAN,    2. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,    3. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,    4. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4. 7. Obsługa Guest VLAN dla IEEE 802.1x 8. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos 9. Wbudowana obrona procesora urządzenia przed atakami DoS 10. Obsługa TACACS+ (RFC 1492) 11. Obsługa RADIUS Authentication (RFC 2865) 12. Obsługa RADIUS Accounting (RFC 2866) 13. RADIUS and TACACS+ per-command Authentication 14. Bezpieczeństwo MAC adresów     1. ograniczenie liczby MAC adresów na porcie     2. zatrzaśnięcie MAC adresu na porcie     3. możliwość wpisania statycznych MAC adresów na port/vlan 15. Możliwość wyłączenia MAC learning 16. Obsługa SNMPv1/v2/v3 17. Klient SSH2 18. Zabezpieczenie przełącznika przed atakami DoS     1. Networks Ingress Filtering RFC 2267     2. SYN Attack Protection     3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania 19. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 20. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika 21. Obsługa bezpiecznego transferu plików SCP/SFTP 22. Obsługa DHCP Option 82 23. Obsługa Gratuitous ARP Protection 24. Obsługa Trusted DHCP Server 25. Obsługa DHCP Snooping 26. Obsługa DHCP Secured ARP/ARP Validation 27. Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x 28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s 29. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania 30. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D 31. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w 32. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s 33. Obsługa PVST+ 34. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619 lub ERPS G.8032 35. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów 36. 36. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników. |
|  | Zarządzanie | 1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol) 2. Obsługa synchronizacji czasu NTP 3. Zarządzanie przez SNMP v1/v2/v3 4. Zarządzanie przez przeglądarkę WWW – protokół http i https 5. Telnet Serwer/Klient dla IPv4 / IPv6 6. SSH2 Serwer/Klient dla IPv4 / IPv6 7. Ping dla IPv4 / IPv6 8. Traceroute dla IPv4 / IPv6 9. Obsługa SYSLOG z możliwością definiowania wielu serwerów 10. Sprzętowa obsługa sFlow 11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757) 12. Obsługa RMON2 (RFC 2021) 13. Obsługa skryptów CLI 14. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) 15. Możliwość uruchamiania skryptów     1. Ręcznie     2. O określonym czasie lub co wskazany okres czasu     3. Na podstawie wpisów w logu systemowym |
| **System Zarządzania siecią (Migracja Extreme NMS-ADV-25)** | | |
|  | Wymagania podstawowe | 1. Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.    1. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare    2. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS 2. Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli 3. Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami oraz wszystkimi dostarczonymi punktami dostępowymi. 4. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników 5. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius. 6. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze. 7. Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES 8. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu. 9. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów 10. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów 11. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II 12. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych. 13. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email’a, wysłanie trapu SNMP, wpisu do Syslog’a lub uruchomienie skryptu. 14. Aplikacja musi posiadać wbudowany Syslog serwer. 15. Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps 16. Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych. 17. Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia. 18. Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:     1. Wysłanie e-mail do wskazanej grupy adresowej     2. Wysłanie informacji SYSLOG do wskazanego serwera     3. Wysłanie TRAP SNMP do wskazanego adresu IP     4. Uruchomienie skryptu w systemie operacyjnym Linux     5. Uruchomienie skryptu skonfigurowanego w systemie zarządzającym 19. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera. 20. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora 21. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach. 22. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem     1. połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu     2. konfiguracji sieci VLAN 23. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https 24. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:     1. adres IP urządzenia     2. adresu MAC urządzenia     3. nazwy urządzenia     4. wersji oprogramowania     5. wersji bootrom     6. lokalizacji urządzenia     7. danych kontaktowych administratora     8. numeru seryjnego     9. numeru inwentaryzacyjnego – własna numeracja 25. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:     1. możliwość automatycznej periodycznej realizacji backup’u konfiguracji urządzeń o wskazanym czasie     2. możliwość realizacji backup’u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych     3. możliwość odtworzenia wskazanej konfiguracji urządzenia     4. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami     5. możliwość obsługi backup’u urządzeń sieciowych różnych producentów 26. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie 27. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach 28. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych. 29. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp. 30. Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:     1. przyłączenia do sieci VLAN     2. przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,     3. konfiguracji Quality of Service     4. konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4     5. możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej. 31. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:     1. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).     2. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).     3. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.     4. generowanie raportów 32. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.     1. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).     2. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax     3. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:  * adres IP kontrolera * liczba obsługiwanych klientów * szczytowe wartości zajmowanego pasma * wersja oprogramowania   1. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje: * adres IP punktu dostępowego * MAC adres punktu dostępowego * wersja oprogramowania * typ punktu dostępowego * kanały pracy poszczególnych interfejsów radiowych * szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych   1. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje: * adres IP klienta * MAC adres klienta * nazwa użytkownika * nazwa punktu dostępowego, do którego dołączony jest użytkownik * BSSID, do którego dołączony jest użytkownik * SSID, do którego dołączony jest użytkownik   1. Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:      + zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).      + zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych  1. Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:    1. adresu MAC    2. adresu IP    3. nazwy komputera    4. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.    5. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.    6. adres IP urządzenia, do którego dołączony jest klient.    7. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.    8. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.    9. nazwa przydzielonej polityki bezpieczeństwa. 2. System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp. 3. System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa 4. System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:    1. Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.    2. Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.    3. Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC    4. Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.    5. Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia 5. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp. 6. Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń. 7. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci. 8. System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS 9. System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp. 10. System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy. 11. System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa. 12. System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:     1. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.     2. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.     3. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android     4. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa     5. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp. 13. System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication 14. System zarządzania musi posiadać przy współpracy z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej 15. Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji. 16. Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji. 17. System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos 18. System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji. 19. Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji. 20. System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp. 21. System Analityki musi zapewniać możliwość tworzenia raportów. 22. System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail. 23. System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością. 24. System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora) 25. System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie. 26. System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu 27. System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki 28. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:     1. Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall, np. Palo Alto, Fortinet, Checkpoint     2. Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny     3. Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – np. Microsoft Intune, AirWatch MDM 29. W momencie dostawy 30. W momencie dostawy system zarządzania musi obsługiwać min. 12 urządzeń 31. W momencie dostawy system zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę urządzeń musi zapewniać obsługę min. 1000 urządzeń klienckich (adresów MAC) 32. W przypadku jeżeli wymienione funkcjonalności ograniczone są subskrypcją czasową, należy dostarczyć taką subskrypcję na okres min. 1 roku 33. Wszystkie dostarczone systemy muszą być objęte kontraktem serwisowym producenta na okres min. 1 roku |
| **System kontroli dostępu administracyjnego, zarządzania uprawnieniami i zgłoszeniami serwisowymi.** | | |
|  | Wymagania ogólne | 1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy. 2. Oprogramowanie musi być w pełni zarządzane przez interfejs WWW za pomocą popularnych przeglądarek internetowych (minimalnie Chrome, Edge, Firefox). 3. Oprogramowanie musi posiadać dynamiczny interfejs użytkownika oparty o konfigurowalne panele oraz widgety w obrębie każdego zalogowanego użytkownika systemu 4. Oprogramowanie musi posiadać logikę zarządzania poprzez reguły (graficzny kreator zdarzeń wyzwalających – warunki oraz akcje) 5. Oprogramowanie musi posiadać otwarte i udokumentowane API komunikacyjne 6. Oprogramowanie w zakresie serwera aplikacji musi współpracować z dystrybucjami Linux (min. Ubuntu Server) lub Windows Server (min. 2012R2) 7. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control). 8. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019 oraz bazą Postgree 9. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java. 10. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie przypisywania wybranych jednostek organizacyjnych, Jednostek lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty. 11. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU. 12. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego. 13. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.ubunt 14. Oprogramowanie musi umożliwiać na automatyczne utworzenie relacji pracownik – komputer na podstawie atrybutu Managed By (z obiektu typu komputer) odczytanym podczas synchronizacji z Active Directory 15. Oprogramowanie musi umożliwiać na automatyczne utworzenie relacji pracownik – przełożony na podstawie atrybutu Manager (z obiektu typu użytkownik) odczytanym podczas synchronizacji z Active Directory 16. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej. 17. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej. 18. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami. |
|  | Baza danych zarządzania konfiguracją | 1. Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI) 2. Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe 3. Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI 4. Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny 5. Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI 6. Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji 7. Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej 8. Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji 9. Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami 10. Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji 11. Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV) 12. Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji 13. Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów 14. Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej 15. Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji |
|  | Zarządzanie zasobami | 1. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami. 2. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu. 3. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów. 4. Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów. 5. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem. 6. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych. 7. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu. 8. Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu 9. Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF 10. Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków 11. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji 12. Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu 13. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej. |
|  | Zarządzanie zgłoszeniami | 1. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:  * Zarządzanie problemem * Zarządzanie incydentem * Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy) * Zarządzanie umowami serwisowymi * Definicje poziomów SLA (reakcja, naprawa, reklamacja)  1. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora. 2. Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika. 3. Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski). 4. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień. 5. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu. 6. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP. 7. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń. 8. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu. 9. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia. 10. Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem. 11. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika. 12. Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika. 13. Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego. 14. Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu. 15. Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników. 16. Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika. 17. Oprogramowanie musi umożliwiać tworzenie szablonów zadań. 18. Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna. 19. Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu. 20. Oprogramowanie musi umożliwiać edycję szablonów powiadomień email. 21. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii. 22. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika. 23. Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia. 24. Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika. 25. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści. 26. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników. 27. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera). 28. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika). 29. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń. 30. Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii. 31. Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika. 32. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem. 33. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego. 34. Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem. 35. Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji 36. mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem. 37. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk). 38. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia). 39. Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia. 40. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc) 41. Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:  * Zmiana statusu po przejęciu zgłoszenia przez opiekuna. * Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna. * Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia. * Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika. * Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika. * Zamykanie zgłoszenia po upływie czasu reklamacji. * Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów. * Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza. * Walidacja zamkniętych zadań w zamykanym zgłoszeniu. * Systemowe potwierdzanie realizacji zgłoszenia. * Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.  1. Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń. 2. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników. 3. Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email. 4. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna). 5. Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika 6. Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia 7. Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń) 8. Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem 9. Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB 10. Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku) 11. Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia 12. Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia 13. Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja) 14. Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu 15. Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą 16. Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności 17. Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu 18. Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa. |
|  | Zarządzanie wnioskami | 1. Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych). 2. Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika. 3. Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu. |
|  | Zarządzanie uprawnieniami | 1. Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych 2. Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych 3. Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych) 4. Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych 5. Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek 6. Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych 7. Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu) 8. Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku 9. Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika) 10. Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób 11. Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych 12. Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika |
|  | Wymagania formalne | 1. Dostarczone licencje na oprogramowanie muszą być bezterminowe. 2. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta. 3. W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu. 4. Zamawiający wymaga od wykonawcy, aby w terminie 30 dni od podpisania umowy przeprowadził wdrożenie systemu w siedzibie zamawiającego/zdalnie |
| **Rozbudowa Macierzy Huawei** | | |
| Szpital posiada obecnie Macierz Huawei / OceanStor 2200 V3 wraz z półką V3E-S-2CEXP25-AC. Realizacja dotyczy rozbudowy macierzy o cztery następujące dyski: | | |
|  | Dysk twardy | 02350TLR L1-L-NLSAS8T 8TB 7.2K RPM NL-SAS Disk Unit(3.5") |
| **Certyfikowane szkolenia z zakresu posiadanych przełączników Extreme (NMS + NAC)** | | |
| Dostawa Vouchera dla trzech osób z zakresu konfiguracji / wdrożenia oraz obsługi posiadanych przez Zamawiającego przełączników oraz systemu Zarządzania NMS-ADV-25 firmy ExtremeNetworks  Voucher powinien zawierać następujące szkolenia certyfikowane oraz mieć możliwość realizacji w ciągu 6-u miesięcy. | | |
|  | NAC – Control: | * + - * SNMP3 Configuration       * Extreme Management Configuration       * Policy Roles, Services & Rules       * Policy Manager Integration       * Initial Extreme Control Setup and Port Configuration       * Extreme Control – Detect Only (Passive Extreme Control)       * Authentication via RADIUS Proxy       * Extreme Control Rules       * End-System Monitoring       * Policy Based Routing Configuration       * Customized Portal       * Guest Access Registration       * Registration Administration       * Authenticated Web Registration * • Agent-Less Assessment without Remediation |
|  | NMS – Management Centre: | * + - * Lab 1: XMC Server Administration       * Lab 2: Integration with XMC       * Lab 3: XMC Device Configuration       * Lab 4: Using XMC for Device Configuration       * Lab 5: Workflows       * Lab 6: XMC Maps       * Lab 7: Managing Firmware       * Lab 8: Managing Configurations       * Lab 9: Governance       * Lab 10: XMC Statistics Collection       * Lab 11: Application Analytics       * Lab 12: Searching with Compass       * Lab 13: FlexViews       * Lab 14: Syslog Events       * Lab 15: Alarms       * Lab 16: SNMP Traps       * Lab 17: Visual Fault Management       * Lab 18: Extreme Management Center – Reporting       * Lab 19: Policy * • Lab 20: Extreme Control – End System Management |
|  |  |  |

## Usługa wdrożenia systemu kontroli dostępu do sieci

W ramach wdrożenia systemu NAC – jako lokalnego systemu dostępu do sieci - działającego wraz z kontrolerem domeny Windows AD przyjmuje się następujące wymagania ogólne, dotyczące zaproponowanych rozwiązań sieciowych:

1. Struktura fizyczna zintegrowanej sieci LAN, na potrzeby podłączania poszczególnych systemów teletechnicznych, jak również użytkowników i systemów innych systemów wykorzystywanych w Szpitalu, biorąc pod uwagę między innymi różną rolę do spełnienia, jak również różne delegacje uprawnień w ramach infrastruktury sieciowej, zakłada się, że składa się z:

* warstwy agregująco-szkieletowej, która jednocześnie jest wykorzystywana na potrzeby wydajnego podłączenia serwerów i systemów zarządzania infrastrukturą sieciową,
* warstwy dostępowej (urządzenia z PoE spełniające role zasilania AP),
* urządzeń już posiadanych przez Szpital – przełączniki dostępowe, które muszą zostać podłączone do urządzeń agregujących oraz mają być zarządzane poprzez System Zarzadzania Siecią (NMS) oraz chronione poprzez System Kontroli Dostępu (NAC),
* Obecnie szpital posiada następujące przełączniki sieciowe:

- ExtremeNetwork x690-48T

- ExtremeNetwork x590-48T

- ExtremeNetwork Series 200 (24 port jak i 48 port)

- Kontroler WIFI – WS-V2110-10-ROW wraz z 80 AP - WS-AP3915i-ROW

W ramach projektu planuje się wdrożenie systemu zarządzania i monitorowania siecią teleinformatyczną oraz uruchomionymi w sieci usługami. Zasadniczymi zadaniami systemu będą monitorowanie stanu infrastruktury, centralizacja procesów zarządzania i konfiguracji urządzeń sieciowych, kontrolowanie i uwierzytelniania podłączających się do infrastruktury urządzeń końcowych oraz monitorowanie usług i aplikacji działających w sieci.

Wdrożenie systemu NAC jego instalacja na serwerach oraz uruchomienie na wskazanych przez zamawiającego switchach powinna odbywać się w godzinach popołudniowych a jego kluczowe uruchomienie w godzinach nocnych w trakcie których będzie minimalny wpływ na działalność Szpitala.

Przed przystąpieniem do realizacji należy wraz z pracownikami działu IT Szpitala przygotować projekt segmentacji sieci VLAN oraz uzgodnić wszelkie polityki jakie będą stosowane dla pracowników Szpitala z kontrolera domeny.

W ramach realizacji oczekuje się dostarczenia zestawu zintegrowanych wzajemnie narzędzi stanowiących jednolity system zarządzania infrastrukturą sieciową. Systemem zarządzania objęte zostaną wszystkie urządzenia przewodowej sieci dostępowej, urządzenia sieci szkieletowej, urządzenia bezprzewodowej sieci WLAN oraz systemy zabezpieczeń sieciowych (takie jak zapora sieciowa firewall - NGFW).

System stanowić będzie centralny punkt zarządzania infrastrukturą sieciową poprzez graficzny interfejs WWW. System zarządzania wykorzystywany będzie do konfiguracji urządzeń infrastruktury dostępowej i szkieletowej, wdrażania w nich konfiguracji lokalnych sieci VLAN, śledzenia atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć. Wymaga się, aby system umożliwiał podgląd i modyfikacje parametrów wszystkich portów urządzeń sieciowych w zakresie konfiguracji przepustowości, sieci VLAN, metody autentykacji i parametrów protokołu Spanning Tree. System musi w sposób automatyczny wykrywać i lokalizować urządzenia podłączone do sieci, przechowywać ich atrybuty i raportować o ich stanie. System musi prowadzić zautomatyzowaną inwentaryzację urządzeń pracujących w sieci, w szczególności na zarządzanie spisem infrastruktury oraz dokumentacji i aktualizacji danych na temat zmian w infrastrukturze. System wykorzystywany będzie do administracji urządzeniami na poziomie plików konfiguracyjnych, planowania aktualizacji oprogramowania firmware, archiwizacji danych konfiguracyjnych, śledzenia wprowadzanych zmian w konfiguracji oraz przywracania konfiguracji.

System musi pozwalać na automatyczne generowanie reprezentacji wizualnej połączeń sieciowych tworząc mapy topologii sieci. Oczekuje się również, że rozwiązanie będzie umożliwiało graficzną lokalizację podłączonych urządzeń końcowych. W przypadku przewodowej sieci LAN musi być jednoznaczne wskazanie urządzenia i portu, do którego podłączone jest urządzenie wraz ze wskazaniem go na mapie. Lokalizacja urządzeń sieci bezprzewodowej WLAN musi jednoznacznie wskazać punkt dostępowy do którego podłączone jest aktualnie urządzenie oraz jego przybliżoną lokalizację w formie graficznej.

System będzie centralnym punktem konfiguracji, wdrażania i egzekwowania polityk bezpieczeństwa zarówno dla przewodowej sieci LAN, jak i systemów podłączonych do bezprzewodowej sieci WLAN.

System posłużyć ma do aktywnego przyznawania dostępu do infrastruktury sieciowej określonym użytkownikom i urządzeniom końcowym w oparciu o informacje pochodzące z serwera usług katalogowych Active Directory poprzez przyznawanie określonego profilu bezpieczeństwa chroniąc tym samym infrastrukturę przed nieautoryzowanym dostępem do zasobów sieciowych. System kontroli dostępu musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci z wykorzystaniem protokołu **IEEE 802.1X lub adresu MAC urządzenia** **i formularza WEB w przypadku dostępu gościa dla sieci WIFI** (w zależności od potrzeb Szpitala)

System ma służyć do uwierzytelniania:

* komputerów użytkowników,
* użytkowników (w przypadku współdzielonych urządzeń),
* drukarek sieciowych,
* telefonów IP,
* Urządzeń Medycznych
* Tabletów, etc…

System musi zapewniać automatyczne wykrywanie punktów końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i adresów IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, Kerberos) lub żądania RADIUS pochodzących z przełączników dostępowych. Wymaga się, aby dostarczony system umożliwiał wyświetlenie w pojedynczym widoku następujących informacji na temat podłączonego systemu końcowego:

* przypisany adres IP,
* fizyczny adres MAC urządzenia,
* nazwa użytkownika (jeżeli występuje),
* adres IP przełącznika, do którego podłączone jest urządzenie końcowe
* port przełącznika, do którego podłączone jest urządzenie końcowe,
* metoda wykorzystana do uwierzytelniania systemu końcowego,
* stan autoryzacji systemu końcowego,
* czas pierwszego podłączenia się do sieci,
* czas ostatniego podłączenia się do sieci.

**Zadanie nr 1**

Cena netto...........................................................................................................zł

(słownie: ..............................................................................................................)

podatek VAT.......................................................................................................zł

Cena brutto..........................................................................................................zł

(słownie: ...............................................................................................................)

w tym:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa asortymentu | Producent, typ/  Model oferowanego sprzętu | Ilość | Cena netto | Cena brutto | Stawka Podatku Vat | Wartość netto  ( Ilość x Cena netto) | Wartość brutto  ( Wartość netto x Stawka Vat) |
| 1. | Oprogramowanie Antywirusowe oraz sprzętowe wraz z procedurami bezpieczeństwa sieciowego |  | 1500 stacji /800 użytkowników  10 serwerów Windows |  |  |  |  |  |
| 2. | Przełącznik Dostępowy |  | 5 szt |  |  |  |  |  |
| 3. | System Zarządzania siecią (Migracja z Extreme NMS-ADV-25) wraz z Systemem kontroli dostępu do sieci |  | 1 szt wraz z licencjami |  |  |  |  |  |
| 4. | Wdrożenie Systemu kontroli dostępu do sieci |  | 1 szt |  |  |  |  |  |
| 5. | System kontroli dostępu administracyjnego, zarządzania uprawnieniami (IAM/IDM) i zgłoszeniami serwisowymi. |  | 1 szt wraz z licencjami na5 agentów i 500 stacji roboczych |  |  |  |  |  |
| 6. | Rozbudowa Macierzy Huawei |  | 1 szt |  |  |  |  |  |
| 7. | Certyfikowane szkolenia z zakresu posiadanych przełączników Extreme (NMS + NAC + Fabric) |  | 3 szt |  |  |  |  |  |
| 8. | Wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym |  | 1 szt |  |  |  |  |  |
| Razem | | | | | | |  |  |

# **Zadanie nr 2**

# **Wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym oraz realizacja audytów bezpieczeństwa.**

## Wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym

**OPRACOWANIE I WDROŻENIE DOKUMENTACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)** w skład której wchodzą następujące dokumenty:

1. Zakres Systemu Zarządzania Bezpieczeństwem Informacji
2. Polityka Systemu Zarządzania Bezpieczeństwem Informacji
3. Cele SZBI
4. Metodyka szacowania i postępowania z ryzykiem

* Tabela szacowania ryzyka
* Tabela postępowania z ryzykiem
* Raport z szacowania i postępowania z ryzykiem

1. Deklaracja stosowania.
2. Plan postępowania z ryzykiem
3. Plan szkoleń i uświadamiania
4. Procedura zarządzania dokumentami i rejestrami
5. Ocena skuteczności zabezpieczeń
6. Procedura audytów wewnętrznych

* Harmonogram audytów
* Raport z audytu wewnętrznego
* Lista kontrolna audytu wewnętrznego SZBI

1. Protokół z przeglądu SZBI
2. Procedura działań korygujących

* Raport z działań korygujących

1. Polityka użytkowania własnych urządzeń elektronicznych
2. Polityka użytkowania urządzeń mobilnych i telepracy
3. Rejestr aktywów:

* Polityka akceptowalnego użytkowania aktywów

1. Polityka klasyfikacji informacji
2. Polityka kontroli dostępu:

* Polityka zarządzania hasłami

1. Polityka stosowania zabezpieczeń kryptograficznych
2. Polityka czystego biurka i czystego ekranu
3. Polityka usuwania i niszczenia informacji
4. Procedury pracy w strefach bezpiecznych
5. Procedury operacyjne dla systemów teleinformatycznych
6. Polityka zarządzania zmianami
7. Polityka zarządzania kopiami zapasowymi
8. Polityka przekazywania informacji
9. Zobowiązanie do zachowania poufności informacji
10. Zobowiązanie do stosowania polityk i procedur SZBI
11. Polityka bezpiecznego rozwoju systemów:

* Specyfikacja wymagań dla systemu przetwarzania informacji

1. Polityka bezpieczeństwa dotycząca dostawców:

* Klauzule bezpieczeństwa dla dostawców i partnerów

1. Procedura zarządzania incydentami:

* Dziennik incydentów

1. Plan odtworzenia po katastrofie
2. Procedura identyfikacji wymagań prawnych i regulacyjnych:

* Wykaz wymagań prawnych i regulacyjnych.

OPRACOWANIE I WDROŻENIE DOKUMENTACJI SYSTEMU ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA (SZCD)w skład której wchodzą następujące dokumenty:

1. Zakres Systemu Zarządzania Ciągłością Działania
2. Polityka Systemu Zarządzania Ciągłością Działania
3. Cele Systemu Zarządzania Ciągłością Działania
4. Metodyka szacowania i postępowania z ryzykiem

* Tabela szacowania ryzyka
* Tabela postępowania z ryzykiem
* Raport z szacowania i postępowania z ryzykiem

1. Plan szkolenia i uświadamiania
2. Procedura audytów wewnętrznych

* Harmonogram audytów
* Raport z audytu wewnętrznego
* Lista kontrolna audytu wewnętrznego SZBI

1. Protokół z przeglądu SZBI
2. Procedura działań korygujących

* Raport z działań korygujących

1. Metodyka analizy wpływu na działalność BIA:

* Kwestionariusz analizy wpływu na działalność

1. Strategia ciągłości działania:

* Lista działań
* Priorytety odtwarzania działań
* Docelowe okresy odtworzenia działań
* Scenariusze incydentów
* Strategia odtwarzania działań

1. Plany ciągłości działania:

* Plan reagowania na incydenty
* Dziennik incydentów
* Lista obiektów służących zachowaniu ciągłości działania
* Plan transportu
* Kluczowe kontakty
* Plan odtworzenia po katastrofie
* Plan odtworzenia działań

1. Plan ćwiczeń i testów:

* Formularz - Raport z ćwiczeń i testów
* Plan obsługi i przeglądów SZCD

1. Formularz przeglądu po incydencie
2. Procedura identyfikacji wymagań prawnych i regulacyjnych:

* Wykaz wymagań prawnych i regulacyjnych.

**Zintegrowanie wspólnej dokumentacji w zakresie spełnienia wymagań normatywnych ISO/IEC 27001 i ISO 22301:**

1. Zakres Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania
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

1. Metodyka szacowania i postępowania z ryzykiem

* Tabela szacowania ryzyka.
* Tabela postępowania z ryzykiem

1. Raport z szacowania i postępowania z ryzykiem
2. Plan szkolenia i uświadamiania
3. Procedura audytów wewnętrznych
4. Harmonogram audytów

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

1. Protokół z przeglądu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania
2. Procedura działań korygujących

* Raport z działań korygujących

1. Procedura identyfikacji wymagań prawnych i regulacyjnych
   * Wykaz wymagań prawnych i regulacyjnych
2. Procedura niezwłocznego podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
3. Procedura stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.
4. Procedura obsługi incydentu;
5. Procedura zapewnienia dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań
6. Procedura klasyfikacji incydentu jako poważnego na podstawie progów uznawania incydentu za poważny;
7. Procedura zgłaszania incydentu poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
8. Procedura współdziałania podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
9. Procedura usuwania podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

Wdrażany System zarządzania bezpieczeństwem w systemie informacyjnym ma spełniać wymagania stawianym Podmiotom będącym Operatorami Usług Kluczowych.

## Audyt Bezpieczeństwa

Celem audytu jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu prac objętych zamówieniem, zgodnie z zarządzeniem nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r.

Przeprowadzony audyt ma wykazać czy został podniesiony poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak.

Raport z audytu musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane w ramach dofinansowania środki wpłynęły na podniesienie poziomu bezpieczeństwa.

**Obszary Audytu:**

1. Ocena skuteczności działania infrastruktury:

* urządzenia i konfiguracja w zakresie ochrony poczty,
* urządzenia i konfiguracja w zakresie ochrony sieci,
* urządzenia i konfiguracja w zakresie systemów serwerowych,
* urządzenia i konfiguracja w zakresie stacji roboczych,
* urządzenia i konfiguracja w zakresie systemów bezpieczeństw.

1. Zarządzanie bezpieczeństwem informacji:

* nośniki wymienne - udokumentowany sposób postępowania,
* zarządzanie tożsamością / dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,
* pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

1. 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.

1. 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.

1. 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.

1. 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.

**Kryteria Audytu Bezpieczeństwa oparte będą o:**

1. Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa.
2. Wymagania normatywne PN-EN ISO/IEC 27001:2017-06.
3. Wymagania normatywne PN-EN ISO 22301:2020-04.
4. Wewnętrzną dokumentację świadczeniodawcy.
5. Przepisy o Krajowym Systemie Cyberbezpieczeństwa.
6. Standardy Krajowych Ram Interoperacyjności (KRI).

**Kwalifikacje jednostki wymagane do przeprowadzenia audytu bezpieczeństwa:**

O udzielenia zamówienia mogą ubiegać się Wykonawcy nie podlegający wykluczeniu i spełniający warunki udziału w postepowaniu, tj.:

1. **posiadający uprawnienia do wykonywania określonej działalności:**
   1. Wykonawca musi posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu €. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
2. **posiadający co najmniej dwóch audytorów posiadających:**
   1. certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
   2. co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
   3. 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.
* 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 Exp

**Zadanie nr 2**

Cena netto...........................................................................................................zł

(słownie: ..............................................................................................................)

podatek VAT.......................................................................................................zł

Cena brutto..........................................................................................................zł

(słownie: ...............................................................................................................)

w tym:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa asortymentu | Producent, typ/  Model oferowanego sprzętu | Ilość | Cena netto | Cena brutto | Stawka Podatku Vat | Wartość netto  ( Ilość x Cena netto) | Wartość brutto  ( Wartość netto x Stawka Vat) |
| 1. | Audyt Bezpieczeństwa |  | 1 szt. |  |  |  |  |  |
| Razem | | | | | | |  |  |

**Załącznik nr 5 do SWZ**

**Klauzula informacyjna dotycząca przetwarzania danych osobowych**

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

• administratorem Pani/Pana danych osobowych jest Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach, ul. Bema 1, 24-100 Puławy, NIP: 7162238942, REGON: 431205731

• w sprawach związanych z Pani/Pana danymi proszę kontaktować się z Inspektorem Ochrony Danych, kontakt pisemny za pomocą poczty tradycyjnej na adres: Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach, ul. Bema 1, 24-100 Puławy, pocztą elektroniczną na adres e-mail: odo@szpitalpulawy.pl;

• Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywający na Zamawiającym;

• odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy Pzp;

• 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;

• obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje nie podania określonych danych wynikają z ustawy Pzp;

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

• Posiada Pan/Pani:

− na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

− na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia 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.

− na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony prawnej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego, a także nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia.

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

• nie przysługuje Pani/Panu:

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

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

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

1. Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy.

……………………………………. ………………………………

Miejscowość, data podpis osoby upoważnionej

1. 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). [↑](#footnote-ref-1)