S p e c y f i k a c j a   
W a r u n k ó w Z a m ó w i e n i a  
(SWZ)

Dostawa oprogramowania komputerowego

wraz ze sprzętem komputerowym.

#### Nazwa oraz adres Zamawiającego.

|  |  |
| --- | --- |
| **Zamawiający:** | **Szpital Specjalistyczny w Brzozowie**  **Podkarpacki Ośrodek Onkologiczny**  **tel./fax: 13 4309552, 13 4309552**  **e-mail:onkologia@szpital-brzozow.pl**  **strona internetowa: www.szpital-brzozow.pl**  **NIP: 6861441430** |
| **Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej**  **http://www.szpital-brzozow.pl** | |

#### 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 (Dz. U. z 2019 r., poz. 2019 ze zm.) [zwanej dalej także „ustawa Pzp”].
2. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3. W postępowaniu ma zastosowania art. 274 ustawy Prawo zamówień publicznych.
4. **Warunki udziału w postępowaniu.**

O zamówienie mogą się ubiegać wykonawcy, którzy :

1. ***nie podlegają wykluczeniu;***

Zamawiający stwierdzi spełnianie powyższego warunku na podstawie złożonego przez Wykonawcę oświadczenia o niepodleganiu wykluczenia z postępowania zgodnie ze wzorem stanowiącym załącznik nr 2 do SIWZ.

1. ***spełniają warunki udziału w postepowaniu, dotyczące:***

- **zdolności do występowania w obrocie gospodarczym.**

Zamawiający nie stawia w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać.

**-uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej;**

Zamawiający nie stawia w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać.

**- sytuacji ekonomicznej lub finansowej;**

Zamawiający nie stawia w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać.

**- zdolności technicznej lub zawodowej;**

Zamawiający nie stawia w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać.

Zamawiający oceni, czy wykonawcy którzy przez oferowane dostawy spełniają wymogi określone przez zamawiającego, oraz nie podlegają wykluczeniu z postępowania, na podstawie wymaganych przez zamawiającego dokumentów określonych w punkcie VI i VII specyfikacji.

1. **Opis przedmiotu zamówienia.**

**„****Dostawa oprogramowania komputerowego wraz ze sprzętem komputerowym.”**

**Szczegółowy opis przedmiotu zamówienia określony został w załączniku nr 1 (formularz ofertowy) do swz.**

Jeżeli Wykonawca stwierdzi, że użyte w SWZ i w załącznikach do SWZ normy krajowe lub normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to Zamawiający dopuszcza w tym zakresie rozwiązania równoważne.

Oznacza to, że parametry techniczne tak wskazanych produktów, określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy. Ponadto, w każdym przypadku stwierdzenie, że opis czy też cecha opisanego produktu, która może wskazywać na źródło pochodzenia lub producenta to Wykonawca również jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w SWZ i/lub w załącznikach do SWZ.

Zamawiający nie przewiduje składania ofert częściowych.

Oznaczenie przedmiotu zamówienia wgwspólnego słownika zamówień CPV:48900000-7.

1. Termin i miejsce wykonania przedmiotu zamówienia.
2. Wymagany termin realizacji przedmiotu zamówienia: 45 dni roboczych od daty podpisania umowy.

**VI. Podmiotowe i przedmiotowe środki dowodowe oraz inne dokumenty wymagane przez zamawiającego.**

1. Dokumenty, które Wykonawca zobowiązany jest dostarczyć **wraz z ofertą przetargową:**

1.1. Oświadczenie o niepodleganiu wykluczeniu z postępowania- wzór zawarty jest w załączniku nr 2 do SWZ.

1.2. Oświadczenie dotyczące wielkości przedsiębiorstwa- wzór zawarty jest w załączniku nr 2 do SWZ.

1.3. W przypadku realizacji zamówienia przy udziale podwykonawców należy złożyć oświadczenie wskazujące podwykonawcę i część zamówienia, która będzie przez niego realizowana - wzór zawarty jest w załączniku nr 2 do SWZ.

1.4. Oświadczenie dotyczące RODO- wzór zawarty jest w załączniku nr 2 do SWZ.

1.5. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia pełnomocnictwo osoby reprezentującej wspólnie działających wykonawców, określające postępowanie do którego się odnosi, precyzujące zakres umocowania oraz określające osobę pełnomocnika i wykonawców udzielających pełnomocnictwa. Pełnomocnictwo powinno być podpisane przez wszystkich wykonawców.

1.6.W przypadku, gdy oferta podpisana jest przez pełnomocnika, pełnomocnictwo do podpisania oferty.

2.Poleganie na zasobach innych podmiotów:

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączącego go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu albo odpowiednio wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust. 3, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
5. zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
6. sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
7. czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
8. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt 3) i 4), a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.

**VII. Podstawy wykluczenia.**

1. Z postępowania o udzielenie zamówienia wykluczony zostanie Wykonawca, w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 108 ust. 1 ustawy Prawo zamówień publicznych.
   1. będący osobą fizyczną, którego prawomocnie skazano za przestępstwo:
2. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
3. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
4. 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, (Dz.U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2021r. poz. 523, 1292, 1559 i 2054),
5. 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,
6. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
7. 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. 2012 poz. 769),
8. 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,
9. 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. 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;
   2. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzją 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;
   3. wobec którego orzeczono zakaz ubiegania sią o zamówienia publiczne;
   4. 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;
   5. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy 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.
10. Zamawiający przewiduje wykluczenie wykonawcy na podstawie art. 109 ust. 1 pkt. 4, 7 -10 ustawy Prawo zamówień publicznych:
    1. w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on winnej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
    2. który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nie-należycie wykonał albo długotrwale nienależycie w 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;
    3. 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 wstanie przedstawić wymaganych podmiotowych środków dowodowych;
    4. 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;
    5. 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
11. Z postępowania o udzielenie zamówienia wyklucza się Wykonawcę z zastrzeżeniem art. 110 ust. 2 ustawy Pzp.
12. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia**.**
13. **Konsorcjum.**
    1. W przypadku wnoszenia oferty wspólnej przez dwa lub więcej podmioty gospodarcze (konsorcja/spółki cywilne) oferta musi spełniać wymagania określone w art. 58 ustawy Prawo zamówień publicznych, w tym:
       1. w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, zgodnie   
          z art. 58 ust. 2 ustawy Pzp Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia lub pełnomocnictwo do reprezentowania w postępowaniu i zawarcia umowy. W związku z powyższym niezbędne jest przedłożenie w ofercie dokumentu zawierającego pełnomocnictwo w celu ustalenia podmiotu uprawnionego do występowania w imieniu Wykonawców w sposób umożliwiający ich identyfikację.
       2. W celu wykazania niepodlegania wykluczeniu z postępowania o udzielenie zamówienia wymagane jest załączenie do oferty oświadczenia i przedłożenia dokumentów dla każdego konsorcjanta oddzielnie.

#### Podwykonawcy.

1. Wykonawca, który zamierza powierzyć wykonanie części zamówienia innej firmie (podwykonawcy) jest zobowiązany do:

1) określenia w złożonej ofercie (w załączniku nr 3do SWZ) informacji jaka część przedmiotu zamówienia będzie realizowana przez podwykonawców z podaniem jego danych jeżeli są znane.

2) Za zgodą Zamawiającego Wykonawca może w trakcie realizacji zamówienia zgłosić nowych podwykonawców do realizacji zamówienia.

**X. 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.**

Informacje ogólne:

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się w sposób następujący:

- za pośrednictwem strony internetowej: [**https://ezamowienia.gov.pl**](https://ezamowienia.gov.pl)**,** pełny link znajduje się w ogłoszeniu o zamówieniu - dotyczy złożenia oferty wraz z dokumentami składanymi wraz z ofertą przetargową, zadawanie pytań, składanie wyjaśnień, wzywanie do wyjaśnień dotyczących treści złożonej oferty, uzupełnienie dokumentów itp.

- za pośrednictwem poczty elektronicznej email: wojciech.majkowski@szpital-brzozow.pl w pozostałych przypadkach (np. zadawanie pytań, składanie wyjaśnień, wzywanie do wyjaśnień dotyczących treści złożonej oferty, uzupełnienie dokumentów itp.)

Uwaga: nazwa pliku zawierającego w/w dokumenty powinna zawierać nazwę (firmę) wykonawcy.

1. Zamawiający dopuszcza złożenie ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty.
2. Wzór oferty stanowi załącznik nr 1 do niniejszej Specyfikacji Warunków Zamówienia.
3. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa” a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP).
4. Do oferty należy dołączyć dokumenty określone w części V pkt. 1, które należy złożyć w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
5. Wykonawca może przed upływem terminu do składania ofert wycofać ofertę.
6. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

**XI. Osoby uprawnione do porozumiewania się z Wykonawcami.**

Osobą uprawnioną do porozumiewania się z Wykonawcami w sprawach formalnoprawnych jest:

- mgr Wojciech Majkowski,tel. 13 43 09 587, e-mail: wojciech.majkowski@szpital-brzozow.pl

#### XII. Termin związania z ofertą.

#### 1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert do dnia 09.09.2022 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 oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

**XIII. Wymagania dotyczące wniesienia wadium.**

Wadium nie jest wymagane.

1. **Zabezpieczenie należytego wykonania umowy.**

Zabezpieczenie nie jest wymagane.

1. **Opis sposobu przygotowania oferty.**

1. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010), które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa” a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). 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 udostępnienie. 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 ustawy Pzp.

2. Ofertę wraz z wymaganymi dokumentami należy złożyć w formie elektronicznej lub w postaci elektronicznej opatrzonej elektronicznym podpisem zaufanym lub podpisem osobistym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).

3. Do przygotowania oferty zaleca się wykorzystanie Formularza Oferty, którego wzór stanowi Załącznik nr 1do SWZ. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu Ofertowym.

4. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.

5. Postanowień ust. 4 nie stosuje się do oferty oraz jeżeli przedmiotowy środek dowowdowy służy potwierdzaniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

1. **Sposób oraz termin składania i otwarcia ofert.**
2. Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w formacie danych pdf, .doc, .docx,.rtf,.xps,.odt. lub w formie elektronicznej opatrzona podpisem zaufanym lub podpisem osobistym.
3. Wykonawca po upływie terminu do składania ofert nie może skutecznie  wycofać złożonej oferty.
4. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
5. Termin składania ofert ustala się na dzień: **11.08.2022r. godz.10:00.**
6. Otwarcie ofert nastąpi w dniu **11.08.2022r. o godzinie 10:30.**
7. Otwarcie ofert jest niejawne.
8. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
9. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
10. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
11. cenach lub kosztach zawartych w ofertach.
12. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
13. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

#### XVII. Sposób obliczenia ceny.

1. Oferowaną cenę należy podać w PLN. Przez cenę należy rozumieć cenę w rozumieniu art. 3 ust. 1 pkt. 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz.U. z 2014 r., poz. 915 z późn. zm.).
2. Cenę należy podać z dokładnością do dwóch miejsc po przecinku.
3. Sposób obliczania ceny, jaki wykonawcy powinni przyjąć w ofertach:

Cena jednostkowa netto x ilość = wartość netto + podatek VAT = wartość brutto

1. Przez cenę zamówienia zamawiający rozumie łączną cenę za całość przedmiotu zamówieniastanowiący całkowite wynagrodzenie wykonawcy.
2. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
3. Jeżeli w zaoferowanej cenie są towary których nabycie prowadzi do powstania   
   u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług (VAT) to wykonawca wraz z ofertą składa o tym informację wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku. - **Niezłożenie przez Wykonawcę informacji będzie oznaczało, że taki obowiązek nie powstaje.**
4. W okolicznościach, o których mowa w ust. 6 zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek VAT, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.

**XVIII. Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobuoceny ofert.**

1. Przy wyborze oferty Zamawiający będzie się kierował kryteriamiokreślonymi poniżej.
2. Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu.
3. Za najkorzystniejszą zostanie uznana oferta z najwyższą ilością punktów określonych w kryteriach.
4. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej ilości przyznanych punktów, wezwie 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.
5. 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.
6. Zamawiający wybiera najkorzystniejszą ofertą w terminie związania ofertą określonym w SWZ.
7. 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.
8. W przypadku braku zgody, o której mowa w ust. 7, oferta podlega odrzuceniu, a Zamawiający zwraca sią o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba,że zachodzą przesłanki do unieważnienia postępowania.
9. Kryteria i ich opis:

kryterium waga kryterium

a) cena 60 %

b) termin realizacji zamówienia 40 %

**a) cena**

Maksymalna ilość możliwych do uzyskania punktów: 60 punktów

Przez cenę zamówienia zamawiający rozumie łączną cenę za całość przedmiotu zamówienia, stanowiącą całkowite wynagrodzenie wykonawcy.

Liczbę punktów, jaką uzyskała badana oferta zamawiający obliczy w następujący sposób:

Oferta z najniższą oferowaną ceną brutto „cmin” otrzymuje punktów 60.

Każda inna oferta „c” otrzymuje ilość punktów w kryterium cena wynikającą z wyliczenia wg wzoru

(cmin/c)\*60 = C

cmin – najniższa oferowana cena

c - cena badanej oferty

C - liczba punktów uzyskanych przez ofertę z kryterium cena

(przy przeliczaniu liczbę punktów zamawiający zaokrągla w dół do dwóch liczb po przecinku np. liczba punktów 4,543 zostanie zaokrąglona do 4,54)

Sposób obliczania ceny, jaki wykonawcy powinni przyjąć w ofertach:

cena jednostkowa netto x ilość = wartość netto + podatek vat = wartość brutto

**b) Termin realizacji**

Maksymalna ilość możliwych do uzyskania punktów wg kryterium termin dostawy – 40 punktów.

Zamawiający określa maksymalny termin dostawy na 45 dni robocze od daty podpisania umowy.

W przypadku, gdy wykonawca zaoferuje 45-dniowy termin dostawy otrzyma 20 pkt. w kryterium termin dostawy.

W przypadku gdy wykonawca zaoferuje termin dostawy w przedziale 40-45 dni roboczych (np. 41dni), otrzyma 30 pkt. w kryterium termin dostawy.

W przypadku gdy wykonawca zaoferuje termin dostawy krótszy niż 40dni roboczych(np. 30 dni), otrzyma 40 pkt. w kryterium termin dostawy.

Wykonawca zobowiązany jest zaoferować termin dostawy z dokładnością do dni (np. 25 dni, 40 dni, itp.).

W przypadku, gdy wykonawca nie określi w ofercie terminu dostawy, zamawiający przyjmie termin dostawy dla tej oferty wynoszący 45 dni.

W postępowaniu zwycięży oferta, która w wyniku oceny otrzyma najwyższą sumę punktów uzyskanych w poszczególnych kryteriach i spełni wszystkie wymogi zawarte w ustawie prawo zamówień publicznych i specyfikacji istotnych warunków zamówienia.

**XIX. Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.**

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnie­niem art. 577 ustawy Pzp, w terminie nie krótszym niż 5 dni od dnia przesłania zawiado­mienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało prze­słane przy użyciu środków komunikacji elektronicznej, 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 udzielenie zamówienia złożono tylko jedną ofertą.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie po­informowany przez 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 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.
7. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą zostanie niezwłocznie powiadomiony przez zamawiającego o miejscu i terminie zawarcia umowy.
8. **Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy.**

Wzór umowy sprzedaży stanowi załącznik do SWZ.

1. **Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy.**
2. 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 ustawy Pzp.
3. Odwołanie przysługuje na:
   1. niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowa­niu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
5. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy Pzp, stronom oraz uczestni­kom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Od­woławczej.
6. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” ustawy Pzp.

**XXII. Informacje dodatkowe dotyczące składania ofert.**

1. Niniejsza SWZ oraz wszystkie dokumenty do niej dołączone mogą być użyte jedynie w celu sporządzenia oferty.
2. Wykonawca przedstawia ofertę zgodnie z wymaganiami określonymi w niniejszej SWZ.
3. Wykonawca ponosi wszystkie koszty związane z przygotowaniem i złożeniem oferty Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
4. Zamawiający nie przewiduje składania ofert wariantowych.
5. Zamawiający nie przewiduje aukcji elektronicznej
6. Zamawiający nie przewiduje udzielenie zamówień powtarzających.
7. **Klauzula informacyjna dotycząca RODO.**

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

1. Administratorem danych osobowych Wykonawcy oraz osób, których dane Wykonawca przekazał w niniejszym postępowaniu jest Szpital Specjalistyczny w Brzozowie Podkarpacki Ośrodek Onkologiczny , Im. Ks. B. Markiewicza, 36-200 Brzozów, ul. Ks. J. Bielawskiego 18
2. Z Inspektorem Ochrony Danych można się skontaktować poprzez e-mail [robert.tomza@szpital-](mailto:robert.tomza@szpital-)brzozow.pl, lub pisemnie na adres Administratora.
3. Dane osobowe Wykonawcy przetwarzane będą na podstawie art. 6 ust. 1 lit. CRODO w celu związanym z postępowaniem o udzielenie niniejszego zamówienia publicznego,prowadzonym w trybie przetargu nieograniczonego;
4. Odbiorcami danych osobowych Wykonawcy będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp;
5. Dane osobowe Wykonawcy będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
6. Obowiązek podania przez Wykonawcę danych osobowych bezpośrednio go dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
7. W odniesieniu do danych osobowych Wykonawcy decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8. Wykonawca posiada:

* na podstawie art. 15 RODO prawo dostępu do swoich danych osobowych;
* na podstawie art. 16 RODO prawo do sprostowania danych osobowych, o ile ich zmiana nie skutkuje zmianą wyniku postępowania o udzielenie zamówienia publicznego czy też zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie narusza 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 praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego UE lub państwa członkowskiego;
* prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy Wykonawca uzna, że przetwarzanie jego danych osobowych narusza przepisy RODO;

1. Wykonawcy nie przysługuje:

* 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.

**UWAGA!**

1. Do obowiązków Wykonawcy należą m.in. obowiązki wynikające z RODO, w szczególności obowiązek informacyjny przewidziany w art. 13 RODO względem osób fizycznych, których dane osobowe dotyczą i od których dane te Wykonawca bezpośrednio pozyskał.
2. Jednakże obowiązek informacyjny wynikający z art. 13 RODO nie będzie miał zastosowania, gdy i w zakresie, w jakim osoba fizyczna, której dane dotyczą, dysponuje już tymi informacjami (vide: art. 13 ust. 4 RODO).
3. Ponadto, Wykonawca będzie musiał wypełnić obowiązek informacyjny wynikający z art. 14 RODO względem osób fizycznych, których dane przekazuje Zamawiającemu i których dane pośrednio pozyskał, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.
4. W związku z powyższym Wykonawca składa (o ile dotyczy) stosowne oświadczenie- wzór zawarty jest w załączniku do SWZ.

**ZATWIERDZAM:**

**…………………………………**

**Załącznik nr 1**

Wykonawca:

……………………………

……………………………

……………………………

(*pełna nazwa/firma, adres)*

NIP *……………………….*

**Osoba/y upoważniona/e do kontaktu:**

……………………………………

Nr tel. …………………………….

mail ………………..…………….

**W Z Ó R O F E R T Y**

W odpowiedzi na ogłoszenie dotyczące udzielenia zamówienia publicznego na dostawę oprogramowania wraz ze sprzętem komputerowym, znak sprawy SZSPOO.SZPiGM. 3810/42/2022, przedstawiamy następującą ofertę:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***L.p.*** | ***Opis przedmiotu zamówienia*** | ***j.m.*** | ***Ilość*** | ***Cena jedn. netto PLN*** | ***Wartość netto PLN*** | ***VAT %*** | ***Wartość brutto PLN*** | ***Typ (nazwa, numer katalogowy) /producent*** |
| 1. | Program antywirusowy. | Szt. | 1 |  |  |  |  |  |
| 2. | System do backupu. | Szt. | 1 |  |  |  |  |  |
| 3. | Biblioteka taśmowa. | Szt. | 1 |  |  |  |  |  |
| 4. | System NAC. | Szt. | 1 |  |  |  |  |  |
| 5. | System NAS. | Szt. | 1 |  |  |  |  |  |
| 6. | System UTM. | Szt. | 1 |  |  |  |  |  |
|  | **RAZEM** | | | |  |  |  |  |

Termin dostawy: ………………. dni. (max. 45 dni)

**PARAMETRY OFEROWANEGO SPRZĘTU**

**Należy wpisać parametry sprzętu zaoferowanego przez wykonawcę.**

**Tabela 1. – Program antywirusowy.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany** | | | | | | | **Parametr oferowany**  **Wpisać TAK/NIE lub poziom oferowanego parametru** | | | | | |
| 1 | Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 2 | Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 3 | Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 4 | Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 5 | Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 6 | Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 7 | Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 8 | Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. | TAK, WYMAGANE | | | | | | |  | | | | | |
| 9 | Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). | TAK, WYMAGANE | | | | | | | | |  | | | |
| 10 | Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. | TAK, WYMAGANE | | | | | | | | |  | | | |
| 11 | Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. | TAK, WYMAGANE | | | | | | | | |  | | | |
| 12 | Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. | TAK, WYMAGANE | | | | | | | | |  | | | |
| 13 | Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. | TAK, WYMAGANE | | | | | | | | |  | | | |
| 14 | Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. | TAK, WYMAGANE | | | | | | | | |  | | | |
| 15 | Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. | TAK, WYMAGANE | | | | | | | | | |  | | |
| 16 | Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. | TAK, WYMAGANE | | | | | | | | | |  | | |
| Ochrona stacji roboczych | | | | | | | | | | | | | | |
| 17 | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11). | TAK, WYMAGANE | | | | | | | | | |  | | |
| 18 | Rozwiązanie musi wspierać architekturę ARM64. | TAK, WYMAGANE | | | | | | | | | |  | | |
| 19 | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | TAK, WYMAGANE | | | | | | | | | |  | | |
| 20 | Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. | TAK, WYMAGANE | | | | | | | | | |  | | |
| 21 | Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | TAK, WYMAGANE | | | | | | | | | |  | | |
| 22 | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | TAK, WYMAGANE | | | | | | | | | |  | | |
| 23 | Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 24 | Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 25 | Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 26 | Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). | TAK, WYMAGANE | | | | | | | | | | |  | |
| 27 | Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 28 | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 29 | Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 30 | Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 31 | Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:   * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. | TAK, WYMAGANE | | | | | | | | | | |  | |
| 32 | Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. | TAK, WYMAGANE | | | | | | | | | | | |  |
| 33 | Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. | TAK, WYMAGANE | | | | | | | | | | | |  |
| 34 | Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. | TAK, WYMAGANE | | | | | | | | | | | |  |
| 35 | Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). | TAK, WYMAGANE | | | | | | | | | | | |  |
| 36 | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | TAK, WYMAGANE | | | | | | | | | | | |  |
| 37 | Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 38 | Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:   * tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, * tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, * tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, * tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 39 | Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 40 | Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 41 | Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 42 | Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 43 | Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 44 | Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day | TAK, WYMAGANE | | | | |  | | | | | | | |
| 45 | W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. | TAK, WYMAGANE | | | | |  | | | | | | | |
| Ochrona serwera | | | | | | | | | | | | | | |
| 46 | Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 47 | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 48 | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 49 | Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 50 | Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 51 | Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 52 | Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 53 | Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. | TAK, WYMAGANE | | | | |  | | | | | | | |
| Dodatkowe wymagania dla ochrony serwerów Windows: | | | | | | | | | | | | | | |
| 54 | Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. | TAK, WYMAGANE | |  | | | | | | | | | | |
| 55 | Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). | TAK, WYMAGANE | |  | | | | | | | | | | |
| 56 | Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. | TAK, WYMAGANE | |  | | | | | | | | | | |
| 57 | . Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | TAK, WYMAGANE | |  | | | | | | | | | | |
| 58 | Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | TAK, WYMAGANE | | | | | |  | | | | | | |
| 59 | Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. | TAK, WYMAGANE | | | | | |  | | | | | | |
| 60 | Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. | TAK, WYMAGANE | | | | | |  | | | | | | |
| 61 | Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | TAK, WYMAGANE | | | | | |  | | | | | | |
| 62 | Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. | TAK, WYMAGANE | | | | | |  | | | | | | |
| Dodatkowe wymagania dla ochrony serwerów Linux: | | | | | | | | | | | | | | |
| 63 | Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. | TAK, WYMAGANE | | | | | |  | | | | | | |
| 64 | Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. | TAK, WYMAGANE | | | |  | | | | | | | | |
| 65 | Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. | TAK, WYMAGANE | | | |  | | | | | | | | |
| 66 | Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. | TAK, WYMAGANE | | | |  | | | | | | | | |
| Szyfrowanie | | | | | | | | | | | | | | |
| 67 | System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 68 | System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). | TAK, WYMAGANE | | | | |  | | | | | | | |
| 69 | Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. | TAK, WYMAGANE | | | | |  | | | | | | | |
| 70 | Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. | TAK, WYMAGANE | | | | |  | | | | | | | |
| Inne | | | | | | | | | | | | | | |
| 71 | Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 72 | Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 73 | Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 74 | Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 75 | Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 76 | Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 77 | Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. | TAK, WYMAGANE | | |  | | | | | | | | | |
| 78 | Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. | TAK, WYMAGANE | | | | | | | |  | | | | |
| 79 | Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania. | TAK, WYMAGANE | | | | | | | |  | | | | |
| 80 | Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli. | TAK, WYMAGANE | | | | | | | |  | | | | |
| 81 | Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell. | TAK, WYMAGANE | | | | | | | |  | | | | |
| Licencje, szkolenia | | | | | | | | | | | | | | |
| 82 | Min. 500 licencji działających w okresie min. 36 m-cy licząc od dnia dostarczenia licencji. | TAK, WYMAGANE |  | | | | | | | | | | | |
| 83 | Szkolenie z zakresu administrowania rozwiązaniem – szkolenie w formie zdalnej dla min. 6 osób; min. 14 godzin szkoleniowych/osobę; szkolenie potwierdzone zaświadczeniem. Termin szkoleń do ustalenia z zamawiającym | TAK, WYMAGANE |  | | | | | | | | | | | |

**Tabela 2. – System do backupu.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany** | **Parametr oferowany**  **Wpisać TAK/NIE lub poziom oferowanego parametru** | | | | | | | |
| 1 | Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, | TAK, WYMAGANE |  | | | | | | | |
| 2 | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej | TAK, WYMAGANE |  | | | | | | | |
| 3 | Oprogramowanie musi współpracować z hostami zarządzanymi przez VMwarevCenter oraz pojedynczymi hostami. | TAK, WYMAGANE |  | | | | | | | |
| 4 | Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. | TAK, WYMAGANE |  | | | | | | | |
| 5 | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. | TAK, WYMAGANE |  | | | | | | | |
| 6 | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej | TAK, WYMAGANE |  | | | | | | | |
| 7 | Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków | TAK, WYMAGANE |  | | | | | | | |
| 8 | Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) | TAK, WYMAGANE |  | | | | | | | |
| 9 | Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji | TAK, WYMAGANE |  | | | | | | | |
| 10 | Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. | TAK, WYMAGANE |  | | | | | | | |
| 11 | Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. | TAK, WYMAGANE |  | | | | | | | |
| 12 | Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft AzureBlob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. | TAK, WYMAGANE |  | | | | | | | |
| 13 | Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania | TAK, WYMAGANE |  | | | | | | | |
| 14 | Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. | TAK, WYMAGANE |  | | | | | | | |
| 15 | Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) | TAK, WYMAGANE |  | | | | | | | |
| 16 | Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu | TAK, WYMAGANE |  | | | | | | | |
| 17 | Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API | TAK, WYMAGANE |  | | | | | | | |
| 18 | Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji | TAK, WYMAGANE |  | | | | | | | |
| 19 | Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji | TAK, WYMAGANE |  | | | | | | | |
| 20 | Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania | TAK, WYMAGANE |  | | | | | | | |
| 21 | Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) | TAK, WYMAGANE |  | | | | | | | |
| 22 | Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. | TAK, WYMAGANE |  | | | | | | | |
| 23 | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej | TAK, WYMAGANE |  | | | | | | | |
| 24 | Oprogramowanie musi wykorzystywanaćmechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. | TAK, WYMAGANE |  | | | | | | | |
| 25 | Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych | TAK, WYMAGANE |  | | | | | | | |
| 26 | Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru | TAK, WYMAGANE |  | | | | | | | |
| 27 | Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphanedsnapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora | TAK, WYMAGANE |  | | | | | | | |
| 28 | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. | TAK, WYMAGANE |  | | | | | | | |
| 29 | Oprogramowanie musi posiadać wsparcie dla VMwarevSAN potwierdzone odpowiednią certyfikacją VMware. | TAK, WYMAGANE |  | | | | | | | |
| 30 | Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn | TAK, WYMAGANE |  | | | | | | | |
| 31 | Oprogramowanie musi posiadać wsparcie dla NDMP | TAK, WYMAGANE |  | | | | | | | |
| 32 | Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) | TAK, WYMAGANE |  | | | | | | | |
| 33 | Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. | TAK, WYMAGANE |  | | | | | | | |
| 34 | Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym CatalystCopy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. | TAK, WYMAGANE |  | | | | | | | |
| 35 | Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. | TAK, WYMAGANE |  | | | | | | | |
| 36 | Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzwImmutability) | TAK, WYMAGANE |  | | | | | | | |
| 37 | Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. | TAK, WYMAGANE |  | | | | | | | |
| 38 | Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMwarevSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. | TAK, WYMAGANE |  | | | | | | | |
| 39 | Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMwarevSphere. Dla replikacji ciągłej musi być możliwośc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. | TAK, WYMAGANE |  | | | | | | | |
| 40 | Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik | TAK, WYMAGANE |  | | | | | | | |
| 41 | Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replicaseeding) | TAK, WYMAGANE |  | | | | | | | |
| 42 | Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) | TAK, WYMAGANE |  | | | | | | | |
| 43 | Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. | TAK, WYMAGANE |  | | | | | | | |
| 44 | Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) | TAK, WYMAGANE |  | | | | | | | |
| 45 | Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami | TAK, WYMAGANE |  | | | | | | | |
| 46 | Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre | TAK, WYMAGANE |  | | | | | | | |
| 47 | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków | TAK, WYMAGANE |  | | | | | | | |
| 48 | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft AzureStack oraz Amazon EC2. | TAK, WYMAGANE |  | | | | | | | |
| 49 | Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików | TAK, WYMAGANE |  | | | | | | | |
| 50 | Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. | TAK, WYMAGANE |  | | | | | | | |
| 51 | Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:   * Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs * BSD: UFS, UFS2 * Solaris: ZFS, UFS * Mac: HFS, HFS+ * Windows: NTFS, FAT, FAT32, ReFS * Novell OES: NSS | TAK, WYMAGANE |  | | | | | | | |
| 52 | Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. | TAK, WYMAGANE |  | | | | | | | |
| 53 | Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. | TAK, WYMAGANE |  | | | | | | | |
| 54 | Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. | TAK, WYMAGANE |  | | | | | | | |
| 55 | Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. | TAK, WYMAGANE |  | | | | | | | |
| 56 | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "PermanentlyDeleted Objects"), | TAK, WYMAGANE |  | | | | | | | |
| 57 | Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska | TAK, WYMAGANE |  | | | | | | | |
| 58 | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych | TAK, WYMAGANE |  | | | | | | | |
| 59 | Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska | TAK, WYMAGANE |  | | | | | | | |
| 60 | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych | TAK, WYMAGANE |  | | | | | | | |
| 61 | Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. | TAK, WYMAGANE |  | | | | | | | |
| 62 | Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. | TAK, WYMAGANE |  | | | | | | | |
| 63 | Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego | TAK, WYMAGANE |  | | | | | | | |
| 64 | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN | TAK, WYMAGANE |  | | | | | | | |
| 65 | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA | TAK, WYMAGANE |  | | | | | | | |
| 66 | Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN | TAK, WYMAGANE |  | | | | | | | |
| 67 | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. | TAK, WYMAGANE | | |  | | | | | |
| 68 | Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. | TAK, WYMAGANE | | |  | | | | | |
| 69 | Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem | TAK, WYMAGANE | | | | |  | | | |
| 70 | Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere | TAK, WYMAGANE | | | | |  | | | |
| 71 | Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. | TAK, WYMAGANE | | | | |  | | | |
| 72 | Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. | TAK, WYMAGANE | | | | |  | | | |
| 73 | System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMwarevSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich | TAK, WYMAGANE | | | |  | | | | |
| 74 | System musi umożliwiać monitorowanie środowiska wirtualizacyjnegoVMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie | TAK, WYMAGANE | | | |  | | | | |
| 75 | System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. | TAK, WYMAGANE | | | |  | | | | |
| 76 | System musi mieć status „VMwareReady” i być przetestowany i certyfikowany przez VMware | TAK, WYMAGANE | | | |  | | | | |
| 77 | System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter | TAK, WYMAGANE | | | |  | | | | |
| 78 | System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn | TAK, WYMAGANE | | | |  | | | | |
| 79 | System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel | TAK, WYMAGANE | | | | | |  | | |
| 80 | System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk | TAK, WYMAGANE | | | | | |  | | |
| 81 | System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora | TAK, WYMAGANE | | | | | |  | | |
| 82 | System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów | TAK, WYMAGANE | | | | | |  | | |
| 83 | System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) | TAK, WYMAGANE | | | | | |  | | |
| 84 | System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna | TAK, WYMAGANE | | | | | | |  | |
| 85 | System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego | TAK, WYMAGANE | | | | | | |  | |
| 86 | System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta | TAK, WYMAGANE | | | | | | |  | |
| 87 | System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. | TAK, WYMAGANE | | | | | | |  | |
| 88 | System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. | TAK, WYMAGANE | | | | | | |  | |
| 89 | System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware | TAK, WYMAGANE | | | | | | |  | |
| 90 | System musi mieć możliwość monitorowania instancji VMwarevCloudDirector w wersji 8.x i 9.x | TAK, WYMAGANE | | | | | | |  | |
| 91 | System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 | TAK, WYMAGANE | | | | | | |  | |
| 92 | System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. | TAK, WYMAGANE | | | | | | |  | |
| 93 | System musi być certyfikowany przez VMware i posiadać status „VMwareReady” | TAK, WYMAGANE | | | | | | |  | |
| 94 | System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V | TAK, WYMAGANE | | | | | | |  | |
| 95 | System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF | TAK, WYMAGANE | | | | | | | |  |
| 96 | System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc | TAK, WYMAGANE | | | | | | | |  |
| 97 | System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach | TAK, WYMAGANE | | | | | | | |  |
| 98 | System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów | TAK, WYMAGANE | | | | | | | |  |
| 99 | System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych | TAK, WYMAGANE | | | | | | | |  |
| 100 | System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych | TAK, WYMAGANE | | | | | | | |  |
| 101 | System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury | TAK, WYMAGANE | | | | | | | |  |
| 102 | System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta | TAK, WYMAGANE | |  | | | | | | |
| 103 | System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. | TAK, WYMAGANE | |  | | | | | | |
| 104 | System musi mieć możliwość generowania raportu planowania pojemności (capacityplanning) bazującego na scenariuszach ‘what-if’. | TAK, WYMAGANE | |  | | | | | | |
| 105 | System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware | TAK, WYMAGANE | |  | | | | | | |
| 106 | System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphanedsnapshots) | TAK, WYMAGANE | |  | | | | | | |
| 107 | System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie | TAK, WYMAGANE | |  | | | | | | |
| 108 | Instalacja systemu na powierzonych przez zamawiającego zasobach. | TAK, WYMAGANE | |  | | | | | | |
| 109 | Licencja oprogramowania w wersji wieczystej pozwalająca na obsługę min 50 instancji z możliwością rozbudowy. | TAK, WYMAGANE  - podać ilość instancji | |  | | | | | | |
| 110 | Wsparcie producenta na okres min. 1 roku. | TAK, WYMAGANE  - podać okres wsparcia | | | | | | | |  |

**Tabela 3. – Biblioteka taśmowa.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany** | **Parametr oferowany**  **Wpisać TAK/NIE lub poziom oferowanego parametru** |
| 1 | Dostarczony autoloader wraz z akcesoriami dodatkowymi musi być fabrycznie nowy, dostarczony razem z gwarancją producenta. | TAK, WYMAGANE |  |
| 2 | Autoloader musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19”. | TAK, WYMAGANE |  |
| 3 | Obudowa powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii biblioteki. | TAK, WYMAGANE |  |
| 4 | Autoloader musi być wyposażony w min. 2 magazynki z wnękami dla nośników z taśmą, pozwalające na umieszczenie min. 4 taśm LTO w każdym magazynku. | TAK, WYMAGANE |  |
| 5 | Minimum 8 slotów na taśmy LTO | TAK, WYMAGANE |  |
| 6 | Napęd typu LTO-7 z interfejsem FC | TAK, WYMAGANE |  |
| 7 | FC, min. 8Gb/s | TAK, WYMAGANE |  |
| 8 | Biblioteka musi mieć na obudowie wyprowadzony min. 1 interfejs RJ-45 Ethernet 10/100MB/s do komunikacji z układem zdalnego zarządzania biblioteką | TAK, WYMAGANE |  |
| 9 | Minimum 1 zasilacz | TAK, WYMAGANE |  |
| 10 | Autoloader musi posiadać wbudowany zintegrowany czytnik kodów kreskowych do automatycznej inwentaryzacji i identyfikacji kaset z taśmą magnetyczną. | TAK, WYMAGANE |  |
| 11 | Autoloader   musi posiadać minimum jeden slot typu Import/Export, do wymiany (ładowanie i wyciąganie kasetek z nośnikiem) bez konieczności wyłączania lub przerywania operacji zapisu/odczytu na innych kasetkach znajdujących się w napędach biblioteki). | TAK, WYMAGANE |  |
| 12 | Panel kontrolny/operatora pozwalający wykonywać [m.in](http://m.in). operacje:  - Inwentaryzacja zasobów biblioteki  - Ustawienia i konfiguracja  zainstalowanych napędów  - Ustawienia adresów IP dla modułu zarządzania  - Ustawienia zabezpieczenia dostępu do modułu operatora / panelu kontrolnego poprzez ustawienie hasła lub PIN-u  - Wykonanie testów diagnostycznych poprawności pracy biblioteki i napędów.  - Relokacja nośników danych i nośników czyszczących  - Aktualizacja oprogramowania wewnętrznego.  Panel operatora wyposażony w czytelny wyświetlacz i przyciski umożliwiające sterowanie wyświetlaną informacją.  Układ zdalnego zarządzania pozwalający na zabezpieczanie dostępu do zarządzania biblioteką poprzez wprowadzenie hasła lub   PIN-u.  Układ zdalnego zarządzania umożliwiający zdalne wysuwanie zainstalowanych magazynków. | TAK, WYMAGANE |  |
| 13 | Biblioteka musi umożliwiać zarządzanie i konfigurowanie zasobów sprzętowych poprzez interfejs graficzny uruchamiany z poziomu przeglądarki WWW bez konieczności instalacji dodatkowego oprogramowania na stacji operatora. | TAK, WYMAGANE |  |
| 14 | minimum 36 miesięcy | TAK, WYMAGANE |  |
| 15 | Taśma czyszcząca – 1 sztuka.  Taśm LTO7 - 16 sztuk  taśmy | TAK, WYMAGANE |  |
| 16 | Wykonawca poza dostawą systemu zapewni również jego prawidłowy montaż, rozruch, wstępną konfigurację i przeszkolenie personelu Zamawiającego. | TAK, WYMAGANE |  |

**Tabela 4. – System NAC.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany** | **Parametr oferowany**  **Wpisać TAK/NIE lub poziom oferowanego parametru** | | | | | | | | | | |
| 1 | System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. | TAK, WYMAGANE |  | | | | | | | | | | |
| 2 | System musi współpracować z urządzeniami wielu producentów (tzw. multivendor) | TAK, WYMAGANE |  | | | | | | | | | | |
| 3 | System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. | TAK, WYMAGANE |  | | | | | | | | | | |
| 4 | System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. | TAK, WYMAGANE |  | | | | | | | | | | |
| 5 | System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. | TAK, WYMAGANE |  | | | | | | | | | | |
| 6 | System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. | TAK, WYMAGANE |  | | | | | | | | | | |
| 7 | System musi umożliwiać obsługę co najmniej 1000 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 50000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. | TAK, WYMAGANE |  | | | | | | | | | | |
| 8 | Licencja ma być zwalniana po rozłączeniu urządzenia końcowego. | TAK, WYMAGANE |  | | | | | | | | | | |
| 9 | System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (BringYourOwn Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. | TAK, WYMAGANE |  | | | | | | | | | | |
| 10 | System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:   * 1. VM – min. VMWareESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, CitrixXenServer w wersji min 4.x   2. Maszyny fizyczne - serwery wspierane przez producenta. | TAK, WYMAGANE |  | | | | | | | | | | |
| 11 | System musi posiadać funkcjonalność serwerów:   * 1. serwera RADIUS dla infrastruktury sieciowej,   2. serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,   3. serwera VPN,   4. serwera DNS,   5. serwera SYSLOG,   6. serwera TFTP,   7. serwera TACACS+,   8. serwera Monitoringu,   9. serwera DHCP,   10. serwera polityk uwierzytelniania i kontroli dostępu 802.1X,   11. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. | TAK, WYMAGANE |  | | | | | | | | | | |
| 12 | System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. | TAK, WYMAGANE |  | | | | | | | | | | |
| 13 | System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. | TAK, WYMAGANE |  | | | | | | | | | | |
| 14 | System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. | TAK, WYMAGANE |  | | | | | | | | | | |
| 15 | System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z innych systemów zewnętrznych. | TAK, WYMAGANE |  | | | | | | | | | | |
| 16 | System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. | TAK, WYMAGANE | |  | | | | | | | | | |
| 17 | System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. | TAK, WYMAGANE | |  | | | | | | | | | |
| 18 | System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. | TAK, WYMAGANE | |  | | | | | | | | | |
| 19 | System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie. | TAK, WYMAGANE | |  | | | | | | | | | |
| 20 | Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). | TAK, WYMAGANE | |  | | | | | | | | | |
| 21 | System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. tożsamość, MAC adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. | TAK, WYMAGANE | |  | | | | | | | | | |
| 22 | System musi zapewniać scentralizowane zarządzanie urządzeniami sieciowymi. Zarządzanie musi odbywać się bezagentowo, a w systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia. | TAK, WYMAGANE | |  | | | | | | | | | |
| 23 | System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. | TAK, WYMAGANE | |  | | | | | | | | | |
| 24 | System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych i końcowych za pomocą min. protokołu SNMP. | TAK, WYMAGANE | |  | | | | | | | | | |
| 25 | Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu: VLANów, autoryzacji, statusu, opisu. | TAK, WYMAGANE | |  | | | | | | | | | |
| 26 | System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. | TAK, WYMAGANE | |  | | | | | | | | | |
| 27 | System musi zapewniać funkcjonalność wizualizacji konfiguracji podsieci IP oraz przypisania jej do jednostek. | TAK, WYMAGANE | |  | | | | | | | | | |
| 28 | System musi posiadać funkcję zintegrowanego serwera DHCP. | TAK, WYMAGANE | |  | | | | | | | | | |
| 29 | System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. | TAK, WYMAGANE | |  | | | | | | | | | |
| 30 | System musi wspierać funkcjonalność włączania i wyłączania podsieci IP, adresów IP bez konieczności usuwania ich z systemu. | TAK, WYMAGANE | |  | | | | | | | | | |
| 31 | System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. | TAK, WYMAGANE | |  | | | | | | | | | |
| 32 | System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP. | TAK, WYMAGANE | | | |  | | | | | | | |
| 33 | System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. | TAK, WYMAGANE | | | |  | | | | | | | |
| 34 | System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD). | TAK, WYMAGANE | | | |  | | | | | | | |
| 35 | System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS. | TAK, WYMAGANE | | | |  | | | | | | | |
| 36 | Captive Portal musi umożliwiać obsługę instalacji agentów, dystrybucji certyfikatów użytkowników oraz generowania autokonfiguratorów sieci. | TAK, WYMAGANE | | | |  | | | | | | | |
| 37 | System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia, pobierać certyfikaty, agenty oraz uruchamiać autokonfiguratorów sieci. | TAK, WYMAGANE | | | |  | | | | | | | |
| 38 | Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor. | TAK, WYMAGANE | | | |  | | | | | | | |
| 39 | Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory | TAK, WYMAGANE | | | |  | | | | | | | |
| 40 | Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory | TAK, WYMAGANE | | | | |  | | | | | | |
| 41 | Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). | TAK, WYMAGANE | | | | |  | | | | | | |
| 42 | Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. | TAK, WYMAGANE | | | | |  | | | | | | |
| 43 | System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. | TAK, WYMAGANE | | | | |  | | | | | | |
| 44 | System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego, co najmniej:   * 1. PaloAlto   2. Fortigate   3. Sophos   4. FlowMon   5. ESET NOD32   6. CheckPoint | TAK, WYMAGANE | | | | |  | | | | | | |
| 45 | System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. | TAK, WYMAGANE | | | | |  | | | | | | |
| 46 | System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. | TAK, WYMAGANE | | | | | | |  | | | | |
| 47 | System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych. | TAK, WYMAGANE | | | | | | |  | | | | |
| 48 | System musi obsługiwać metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej:   * 1. DHCP Fingerprinting   2. DHCP SPAN   3. SNMP   4. Vendor OUI   5. TCP   6. Active Directory   7. CDP/LLDP   8. HTTP/S   9. DNS   10. Radius   11. WMI   12. MDM   13. WinRM   14. ONVIF | TAK, WYMAGANE | | | | | | |  | | | | |
| 49 | System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach:   * 1. FortiGate   2. PulseSecure   3. OpenVPN   4. PaloAlto   5. Cisco ASA | TAK, WYMAGANE | | | | | | |  | | | | |
| 50 | System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:   * 1. Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności   2. Czy włączony jest firewall   3. Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur   4. Czy jest włączone szyfrowanie dysku systemowego   5. Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory   6. Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora   7. Czy w systemie są uruchomione procesy wskazane przez administratora   8. Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności   9. Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: * Wartości klucza rejestru * Typuwartości: Number, String, Version | TAK, WYMAGANE | | | | | | |  | | | | |
| 51 | System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. | TAK, WYMAGANE | | | | | | |  | | | | |
| 52 | System musi współpracować z serwerem tokenów. | TAK, WYMAGANE | | | | | | |  | | | | |
| 53 | System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:   * 1. Microsoft Windows   2. Mac OS   3. iOS   4. Android | TAK, WYMAGANE | | | | | | |  | | | | |
| 54 | System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). | TAK, WYMAGANE | | | | | | |  | | | | |
| 55 | System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. | TAK, WYMAGANE | | | | | | |  | | | | |
| 56 | System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:   * 1. wiadomości e-mail,   2. Syslog,   3. notyfikacji systemowych. | TAK, WYMAGANE | | | | | | |  | | | | |
| 57 | System musi zapewniać wsparcie dla obsługi serwerów TACACS+. | TAK, WYMAGANE | | | | | | | |  | | | |
| **Mechanizmy uwierzytelniania** | | | | | | | | | | | | | |
| 58 | System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. | TAK, WYMAGANE | | | | | | | |  | | | |
| 59 | System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:   * 1. MAC,   2. PAP/ASCII,   3. CHAP,   4. SNMP,   5. 802.1X. | TAK, WYMAGANE | | | | | | | |  | | | |
| 60 | wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), itp. | TAK, WYMAGANE | | | | | | | |  | | | |
| 61 | System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. | TAK, WYMAGANE | | | | | | | |  | | | |
| 62 | System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. | TAK, WYMAGANE | | | | | | | |  | | | |
| 63 | System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). | TAK, WYMAGANE | | | | | | | |  | | | |
| 64 | System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:   * 1. Tożsamość/Urządzenie końcowe,   2. Grupa tożsamości/urządzeń końcowych,   3. Parametry urządzeń końcowych, min: system operacyjny, wersja,   4. Atrybuty Active Directory,   5. Jednostka organizacyjna tożsamości/urządzeń końcowych,   6. Urządzenia sieciowe sieci przewodowej, bezprzewodowej,   7. Grupy urządzeń sieciowych,   8. Porty urządzeń sieciowych,   9. Grupy portów urządzeń sieciowych,   10. Jednostka organizacyjna portów,   11. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),   12. Data, czas ważności polityki,   13. Wewnętrzny Captive Portal,   14. Metoda autoryzacji. | TAK, WYMAGANE | | | | | | | |  | | | |
| 65 | System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. | TAK, WYMAGANE | | | | | | | |  | | | |
| 66 | System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. | TAK, WYMAGANE | | | | | | | |  | | | |
| 67 | System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. | TAK, WYMAGANE | | | | | | | |  | | | |
| 68 | System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. | TAK, WYMAGANE | | | | | | | |  | | | |
| 69 | System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. | TAK, WYMAGANE | | | | | | | |  | | | |
| 70 | System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji. | TAK, WYMAGANE | | | | | | | |  | | | |
| 71 | System musi wspierać funkcjonalność różnych typu autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. | TAK, WYMAGANE | | | | | | | |  | | | |
| 72 | System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. | TAK, WYMAGANE | | | | | | | |  | | | |
| 73 | System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP. | TAK, WYMAGANE | | | |  | | | | | | | |
| **Obsługa serwerów certyfikatów CA** | | | | | | | | | | | | | |
| 74 | System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. | TAK, WYMAGANE | | | | | |  | | | | | |
| 75 | Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:   * 1. możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.   2. możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.   3. Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple CertificateEnrollmentProtocol).   4. usługę OCSP (Online Certificate Status Protocol) | TAK, WYMAGANE | | | | | |  | | | | | |
| **Obsługa serwerów VPN** | | | | | | | | | | | | | |
| 76 | System musi posiadać funkcję zintegrowanego serwera VPN oraz zapewniać współpracę z zintegrowanym oraz zewnętrznym serwerem CA. | TAK, WYMAGANE | | | | |  | | | | | | |
| 77 | System musi umożliwiać wystawianie konfiguracji klienckich, certyfikatów dla serwerów VPN. | TAK, WYMAGANE | | | | | |  | | | | | |
| 78 | System musi logować wszelkie próby autoryzacji do serwerów VPN. | TAK, WYMAGANE | | | | | |  | | | | | |
| 79 | System musi zapewniać przynajmniej następujące funkcjonalności serwera VPN:   * 1. Logowanie do zasobów firmy,   2. Obsługę OTP,   3. Przypisanie ustalonego adresu IP. | TAK, WYMAGANE | | | | | |  | | | | | |
| **Obsługa serwerów DNS** | | | | | | | | | | | | | |
| 80 | System musi posiadać funkcję zintegrowanego serwera DNS. | TAK, WYMAGANE | | | | | | |  | | | | |
| 81 | System musi umożliwiać graficzne zarządzanie serwerami DNS. | TAK, WYMAGANE | | | | | | |  | | | | |
| 82 | System musi zapewniać przynajmniej następujące funkcjonalności serwera DNS:   * 1. Zarządzanie strefami,   2. Zarządzanie rekordami stref,   3. Zatwierdzanie przez administratorów moderowanych rekordów stref,   4. Weryfikacja konfiguracji przed instalacją,   5. Instalacja konfiguracji na serwerach DNS | TAK, WYMAGANE | | | | | | |  | | | | |
| **Obsługa serwerów DHCP** | | | | | | | | | | | | | |
| 83 | System musi posiadać funkcję zintegrowanego serwera DHCP. | TAK, WYMAGANE | | | | |  | | | | | | |
| 84 | System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. | TAK, WYMAGANE | | |  | | | | | | | | |
| 85 | System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:   * 1. Uruchamianie usługi dla wybranych podsieci,   2. Przypisanie ustalonego adresu IP dla adresu MAC.   3. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,   4. Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,   5. Możliwość określania braku dostępu dla wybranych adresów MAC,   6. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,   7. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,   8. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,   9. Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,   10. Dokonywanie zmian bez konieczności wyłączania usług | TAK, WYMAGANE | | |  | | | | | | | | |
| **Obsługa serwerów TACACS+** | | | | | | | | | | | | | |
| 86 | System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:   1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. 2. System musi umożliwiać tworzenia haseł administratorom. 3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów 4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. 5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. 6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.   System musi wspierać logowanie administratorów za pomocą tokenów OTP. | TAK, WYMAGANE | | | | | | | | |  | | |
| **Raportowanie i monitoring** | | | | | | | | | | | | | |
| 87 | System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:   1. Monitoring zdarzeń autoryzacji 2. Monitoring dla zdarzeń systemowych. 3. Monitoring dla zdarzeń DHCP. 4. Monitoring dla tożsamości. 5. Monitoring dla urządzeń końcowych. 6. Monitoring dla urządzeń sieciowych 7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. 8. Raport ze zdarzeń logowania z informacją o nadam adresie IP. 9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. 10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. 11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. 12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. 13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. 14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. 15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. 16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.   Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. | TAK, WYMAGANE | | | | | | | | |  | | |
| **Alarmy** | | | | | | | | | | | | | |
| 88 | System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą wiadomości e-mail, Syslog, notyfikacji systemowych. | TAK, WYMAGANE | | | | | | | | | | |  |
| 89 | Alarmy mogą być generowane w sytuacjach, min: Ilości obsługiwanych transakcji RADIUS, opóźnienie obsługi transkacji RADIUS, statusu krytycznego modułów. | TAK, WYMAGANE | | | | | | | | | | |  |
| 90 | System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:   * 1. badanie łączności IP za pomocą ping, traceroute,   2. tcpdump protokołów RADIUS, TACACS+,   3. wyszukiwanie zdarzeń RADIUS z uwzględnieniem nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty, wykonanie zdalnego polecenia na urządzeniu sieciowym. | TAK, WYMAGANE | | | | | | | | | | |  |
| **Wdrożenie i szkolenie** | | | | | | | | | | | | | |
| 91 | dostarczeniu i wdrożeniu rozwiązania typu NAC wraz z oprogramowaniem, niezbędnymi licencjami oraz świadczeniu usługi gwarancji przez okres min. 12 m-cydla wdrożonego systemu. | TAK, WYMAGANE  Podać okres gwarancji | | | | | | | | | |  | |
| 92 | System musi być zainstalowany na infrastrukturze Zamawiającego | TAK, WYMAGANE | | | | | | | | | |  | |
| 93 | Wykonawca przeprowadzi instruktaż dla nie więcej niż 6 pracowników Zamawiającego, który przygotuje wskazanych pracowników do samodzielnego konfigurowania Systemu, operowania Systemem z poziomu administratora oraz użytkownika oraz wykorzystywania Systemu skonfigurowanego w specyficznej infrastrukturze Zamawiającego, w szczególności do samodzielnej konfiguracji Systemu.   * Instruktaż zostanie przeprowadzony w języku polskim * Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy. * Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu * Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą. * Instruktaż będzie realizowany w dni robocze w godzinach 8:00-15:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego.Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu. * Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:   + Architektura produktu   + Poruszanie się po interfejsie użytkownika   + Instalacja konsoli zarządzania i agentów na stacjach końcowych   + Konfiguracja reguł filtrujących/analizujących dla dedykowanego systemu końcowego.   + Wykonanie przykładowych scenariuszy: Konfigurowanie nowych polityk dostępu; Konfigurowanie nowych polityk weryfikacji zgodności stacji końcowych;   + Monitorowanie działania systemu.   + Automatyzacja zadań w tym definiowanie alertów w odpowiedzi na wykryte zdarzenia.   + Manualne uruchamianie zadań.   + Analiza i raportowanie wyników.   + Konfiguracja zadań/reakcji na zdarzenia.   + Zarządzanie użytkownikami i rolami. | TAK, WYMAGANE | | | | | | | | | |  | |

**Tabela 5. – System NAS.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany** | **Parametr oferowany**  **Wpisać TAK/NIE lub poziom oferowanego parametru** |
| 1 | System przeznaczony do instalacji w szafie rack 19” | TAK, WYMAGANE |  |
| 2 | System zapewnia pojemność surową co najmniej 96 TB zbudowaną na min. 12 dyskach. | TAK, WYMAGANE |  |
| 3 | min. 1 procesorem co najmniej 8-rdzeniowy, 64 bitowy, osiągający w testach https://www.cpubenchmark.net/ wynik minimum 19 000. | TAK, WYMAGANE |  |
| 4 | min. 64 GB pamięci RAM z możliwością rozbudowy do min. 128GB w ramach dostarczonego urządzenia. | TAK, WYMAGANE |  |
| 5 | min. 2 porty 10 Gigabit Ethernet optyczne z wkładkami SFP+ MM | TAK, WYMAGANE |  |
| 6 | System umożliwia agregację interfejsów sieciowych, przy czym powinien wspierać min. tryby roundrobin, active backup, 802.3ad | TAK, WYMAGANE |  |
| 7 | System wspiera min. RAID 0,1,5,6, 10, 50, 60 w wersji sprzętowej (dedykowany chipset, który odciąża procesor dla operacji RAID) | TAK, WYMAGANE |  |
| 8 | System umożliwia zdefiniowania z jednej konsoli graficznej systemów plików BTRFS, ZFS, EXT4, XFS, w zależności od zastosowania zasobów dyskowych. | TAK, WYMAGANE |  |
| 9 | System wspieradeduplikację. Jeżeli funkcjonalność wymaga dodatkowej licencji należy ją dostarczyć. | TAK, WYMAGANE |  |
| 10 | System umożliwia uruchomienie wirtualnych maszyn Linux, Windows. | TAK, WYMAGANE |  |
| 11 | System wspiera funkcjonalność kopii migawkowych | TAK, WYMAGANE |  |
| 12 | System integruje się z posiadanym przez Zamawiającego system backupowym VEEAM co najmniej na poziomie funkcjonalności „immutability”. Integracja oznacza, że z poziomu GUI systemu VEEAM ma być możliwość podłączenia systemu jako repozytorium backupowego z możliwością ustawienia funkcjonalności „immutability” | TAK, WYMAGANE |  |
| 13 | System integruje się z posiadanym przez Zamawiającego systemem NAS firmy Infoklinika, co najmniej na poziomie replikacji. W przypadku wątpliwości na etapie weryfikacji, Zamawiający zażąda przedstawienia oświadczenia producenta systemu Forstor o kompatybilności zaoferowanego rozwiązania z systemem Forstor | TAK, WYMAGANE |  |
| 14 | System wspiera funkcjonalność akceleracji zapisów oraz odczytów za pośrednictwem przestrzeni opartej o dyski SSD. Jeżeli funkcjonalność wymaga dodatkowej licencji, nie jest ona przedmiotem postępowania | TAK, WYMAGANE |  |
| 15 | System umożliwia rozbudowę o dodatkową funkcjonalność kopii zapasowych wspierającą co najmniej kopie zapasowe wirtualnych oraz fizycznych maszyn Windows/Linux. Jeżeli funkcjonalność wymaga dodatkowej licencji, nie jest ona przedmiotem postępowania | TAK, WYMAGANE |  |
| 16 | System ma możliwość zarządzania warstwą sprzętową za pośrednictwem dedykowanego portu USB zainstalowanego z przodu urządzenia | TAK, WYMAGANE |  |
| 17 | Maksymalna wysokość systemu: 2U | TAK, WYMAGANE |  |
| 18 | System umożliwia zarządzanie wszystkimi funkcjonalnościami z jednej konsoli administracyjnej poprzez interfejs WWW, z możliwością ustawienia j. polskiego | TAK, WYMAGANE |  |
| 19 | System umożliwia integrację z usługą Active Directory umożliwiającą udostępnianie zasobów w ramach domeny | TAK, WYMAGANE |  |
| 20 | System zapewnia dostęp do zasobów z różnych systemów operacyjnych (Linux, Windows) przy użyciu standardowych protokołów udostępniania plików: NFS (wersja 3 i 4), CIFS/SMB (wersja 2 i 3), oraz protokołu blokowego iSCSI. System musi udostępniać wszystkie usługi protokołu bez dodatkowych licencji i sprzętu | TAK, WYMAGANE |  |
| 21 | System umożliwia rozbudowę o funkcjonalność replikacji. Jeżeli funkcjonalność wymaga dodatkowej licencji, nie jest ona przedmiotem postępowania | TAK, WYMAGANE |  |
| 22 | System zapewnia obsługę alertów, monitorowania i powiadomień mailowych | TAK, WYMAGANE |  |
| 23 | System umożliwia dostęp do szczegółowych informacji o zajętości pamięci, zajętości przestrzeni dyskowej, obciążeniu procesorów, obciążeniu kart sieciowych, temperatury. | TAK, WYMAGANE |  |
| 24 | System objęty gwarancją producenta przez co najmniej 36 miesięcy z czasem naprawy następny dzień. W przypadku awarii dysku, dysk zostaje u Zamawiającego | TAK, WYMAGANE |  |
| 25 | Wykonawca zapewni dostęp do aktualizacji oprogramowania systemu w ramach gwarancji | TAK, WYMAGANE |  |
| 26 | Wykonawca poza dostawą systemu zapewni również jego prawidłowy montaż, rozruch, wstępną konfigurację i przeszkolenie personelu Zamawiającego. | TAK, WYMAGANE |  |

**Tabela 6. – System UTM.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagany** | **Parametr oferowany**  **Wpisać TAK/NIE lub poziom oferowanego parametru** |
| 1 | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. | TAK, WYMAGANE |  |
| 2 | System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. | TAK, WYMAGANE |  |
| 3 | W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. | TAK, WYMAGANE |  |
| 4 | System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. | TAK, WYMAGANE |  |
| 5 | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. | TAK, WYMAGANE |  |
| 6 | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. | TAK, WYMAGANE |  |
| 7 | Monitoring stanu realizowanych połączeń VPN. | TAK, WYMAGANE |  |
| 8 | 1. System realizujący funkcję Firewall musi dysponować minimum:  * 18 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 4 gniazdami SFP+ 10 Gbps. | TAK, WYMAGANE |  |
| 9 | System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB | TAK, WYMAGANE |  |
| 10 | W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę | TAK, WYMAGANE |  |
| 11 | Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B | TAK, WYMAGANE |  |
| 12 | Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps | TAK, WYMAGANE |  |
| 13 | Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps | TAK, WYMAGANE |  |
| 14 | Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps | TAK, WYMAGANE |  |
| 15 | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - IntrusionPrevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Trafficshaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system | TAK, WYMAGANE |  |
| 16 | Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. | TAK, WYMAGANE |  |
| 17 | System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP. | TAK, WYMAGANE |  |
| 18 | W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN | TAK, WYMAGANE |  |
| 19 | Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików | TAK, WYMAGANE |  |
| 20 | Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.   * Amazon Web Services (AWS). * Microsoft Azure * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. | TAK, WYMAGANE |  |
| 21 | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:   * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site. | TAK, WYMAGANE |  |
| 22 | System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:   * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. | TAK, WYMAGANE |  |
| 23 | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM | TAK, WYMAGANE |  |
| 24 | System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. | TAK, WYMAGANE |  |
| 25 | Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. | TAK, WYMAGANE |  |
| 26 | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | TAK, WYMAGANE |  |
| 27 | Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. | TAK, WYMAGANE |  |
| 28 | System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | TAK, WYMAGANE |  |
| 29 | Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). | TAK, WYMAGANE |  |
| 30 | System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. | TAK, WYMAGANE |  |
| 31 | System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). | TAK, WYMAGANE |  |
| 32 | System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. | TAK, WYMAGANE |  |
| 33 | System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. | TAK, WYMAGANE |  |
| 34 | Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | TAK, WYMAGANE |  |
| 35 | Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. | TAK, WYMAGANE |  |
| 36 | System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. | TAK, WYMAGANE |  |
| 37 | Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | TAK, WYMAGANE |  |
| 38 | Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. | TAK, WYMAGANE |  |
| 39 | System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. | TAK, WYMAGANE |  |
| 40 | Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. | TAK, WYMAGANE |  |
| 41 | Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | TAK, WYMAGANE |  |
| 42 | Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | TAK, WYMAGANE |  |
| 43 | Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików | TAK, WYMAGANE |  |
| 44 | Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. | TAK, WYMAGANE |  |
| 45 | Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | TAK, WYMAGANE |  |
| 46 | Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. | TAK, WYMAGANE |  |
| 47 | W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. | TAK, WYMAGANE |  |
| 48 | Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. | TAK, WYMAGANE |  |
| 49 | Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. | TAK, WYMAGANE |  |
| 50 | Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. | TAK, WYMAGANE |  |
| 51 | Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. | TAK, WYMAGANE |  |
| 52 | W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | TAK, WYMAGANE |  |
| 53 | System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. | TAK, WYMAGANE |  |
| 54 | Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. | TAK, WYMAGANE |  |
| 55 | Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. | TAK, WYMAGANE |  |
| 56 | Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | TAK, WYMAGANE |  |
| 57 | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. | TAK, WYMAGANE |  |
| 58 | Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. | TAK, WYMAGANE |  |
| 59 | Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. | TAK, WYMAGANE |  |
| 60 | System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. | TAK, WYMAGANE |  |
| 61 | System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. | TAK, WYMAGANE |  |
| 62 | Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. | TAK, WYMAGANE |  |
| 63 | Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | TAK, WYMAGANE |  |
| 64 | Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. | TAK, WYMAGANE |  |
| 65 | W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. | TAK, WYMAGANE |  |
| 66 | Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. | TAK, WYMAGANE |  |
| 67 | Musi istnieć możliwość logowania do serwera SYSLOG. | TAK, WYMAGANE |  |
| 68 | Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox bazy reputacyjne adresów IP/domena na okres min. 36 miesięcy. | TAK, WYMAGANE podać ilość miesięcy |  |

**Załącznik nr 2 do SWZ**

**Wykonawca:**

……………………………………………………

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

reprezentowany przez:

…………………………………………………

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

Na potrzeby postępowania o udzielenie zamówienia publicznego oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCEPRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA :**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ustawy Pzp w zakresie jaki Zamawiający wymagał.

Oświadczam, **że zachodzą/ nie zachodzą\*** (nie potrzebne skreślić) w stosunku do mnie podstawy wykluczenia wymienione poniżej z postępowania na podstawie art. …………. ustawy Pzp*(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 ustawy Pzp lub art. 109 ustawy Pzp).*Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłemnastępujące środki naprawcze: ……………………………………………………………………………………..……………………………………………………………………

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

**OŚWIADCZENIE DOTYCZĄCE WIELKOŚCI PRZEDSIĘBIORSTWA:**

Na potrzeby postępowania o udzielenie zamówienia publicznego oświadczam, że:

* jestem mikroprzedsiębiorstwem,\*
* jestem małym przedsiębiorstwem,\*
* jestem średnim przedsiębiorstwem,\*
* prowadzę jednoosobowa działalność gospodarczą,\*
* jestem osobą fizyczną nieprowadząca działalności gospodarczej,\*
* inny rodzaj,\*

**\* niepotrzebne skreślić**

**OŚWIADCZENIE DOTYCZĄCE PODYKONAWSTWA**

Oświadczamy, że zaoferowany przedmiot zamówienia wykonamy :

* samodzielnie,\*
* przy udziale podwykonawców,\*

**\* niepotrzebne skreślić**

**W przypadku, gdyWykonawca zamierza powierzyć realizację części zamówienia podwykonawcy uzupełnia poniższą tabelę.**

**Jeżeli wykonawca zamierza wykonać zamówienie samodzielnie nie wypełnia tabelki lub oznacza zapisem w tabelce - nie dotyczy**

|  |  |
| --- | --- |
| Nazwa i adres podwykonawcy | Część zamówienia, którą będzie wykonywał |
|  |  |

**OŚWIADCZENIE DOTYCZĄCE RODO**

Na potrzeby postępowania o udzielenie zamówienia publicznego oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej RODO, wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu (wykonawca wykreśla powyższe oświadczenie w przypadku gdy go nie dotyczy).

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

…………………………………………………………….

(podpis)

**Załącznik nr 3**

Wzór umowy zawierający istotne dla zamawiającego postanowienia, które zostaną wprowadzone do treści zawieranej umowy.

**UMOWA SPRZEDAŻY**

**NR SZPiGM 3810/42/2022**

zawarta w Brzozowie, w dniu …………………….. pomiędzy:

Szpitalem Specjalistycznym w Brzozowie Podkarpackim Ośrodkiem Onkologicznym im. ks. B. Markiewicza, 36-200 Brzozów, ul. Ks. J. Bielawskiego 18, zarejestrowanym w Sądzie Rejonowym w Rzeszowie w Wydziale Gospodarczym Krajowego Rejestru Sądowego pod numerem KRS 0000007954, reprezentowanym przez:

Lek. Tomasza Kondraciuka, MBA - Dyrektora

zwanym w dalszej części umowy „Kupującym”,

a

………………………………………………………………………………………………………………………………,

reprezentowana przez:

……………………………………………………………………….

zwaną w dalszej części umowy „Sprzedającym”.

§ 1

1. Sprzedający sprzedaje a Kupujący kupuje oprogramowanie komputerowewraz ze sprzętem komputerowym. Szczegółowy zakres przedmiotu zamówienia określony jest w ofercie przetargowej stanowiącej załącznik nr 1 do niniejszej umowy, zwany w dalszej części umowy przedmiotem sprzedaży.
2. Sprzedający oświadcza, że przedmiot sprzedaży spełnia wszelkie wymagania norm i przepisów odnoszących się do wyrobów tego typu oraz do ich oznaczenia w sposób wymagany przepisami prawa oraz że Kupujący, ewentualnie podmioty z nim związane mogą przenieść na niego roszczenia wynikające z niespełnienia powyższych wymagań co do jakości produktów lub sposobu ich oznaczania.
3. Sprzedający oświadcza, iż posiada wszelkie wymagane prawem uprawnienia do prowadzenia obrotu przedmiotem umowy, i na każde wezwanie Kupującego niezwłocznie przedstawi dokumenty potwierdzające powyższe.
4. Wykonawca zobowiązany jest do dostawy i wdrożenia przedmiotu zamówienia oraz przeszkolenia personelu w zakresie obsługi programu w terminie do …… dni roboczych od daty podpisania umowy.
5. Każdej ze stron umowy przysługuje prawo wypowiedzenia umowy z zachowaniem 2 tygodniowego terminu wypowiedzenia. W przypadku wypowiedzenia umowy, stronom umowy nie przysługują z tego tytułu roszczenia odszkodowawcze.

§ 2

1. Strony ustalają łączną wartość przedmiotu sprzedaży, określonego w § 1, na kwotę: …………………. PLN brutto (słownie: ……………………………………… ……. /100).
2. Kwota wymieniona w § 2 ust. 1 niniejszej umowy obejmuje wszelkie koszty związane z zakupem oraz przeszkoleniem personelu w zakresie użytkowania przedmiotu zamówienia.
3. Zamawiający przyjmie kompleksową funkcjonalność programu na podstawie protokołu odbioru sporządzonego przez Strony niniejszej umowy.
4. Osobą kontaktową i upoważnioną ze strony Kupującego w sprawie realizacji niniejszej umowy jest Pan Marcin Kolbuch tel. 13 43 09 575.
5. Osobą kontaktową i upoważnioną ze strony Sprzedającego w sprawie realizacji niniejszej umowy jest …………………………….tel./fax. ...................................
6. Wiążąca strony korespondencja w ramach umowy prowadzona będzie w formie pisemnej (adresy siedzib traktuje się jako adresy korespondencyjne), w formie fax. (ze strony Kupującego nr (13) 4309578, ze strony Sprzedającego nr (….) …………. lub w formie email (ze strony Kupującego spożywczy@szpital-brzozow.pl, ze strony Sprzedającego ( ……………………….). Wszelkie uzgodnienia w formie telefonicznej są niewiążące dla stron, strony wykluczają je jako wiążącą formę komunikacji w ramach realizacji umowy.

§ 3

1. Kupujący zobowiązuje się zapłacić za dostarczony przedmiot sprzedaży kwotę ustaloną na podstawie § 2 umowy, przelewem bankowym w terminie do 60 dni od daty otrzymania faktury, przy czym podstawą do przyjęcia faktury jest podpisany przez Strony protokół odbioru.
2. Strony umowy postanawiają, że zapłata należności za dostarczony przedmiot sprzedaży nastąpi z chwilą obciążenia rachunku bankowego Kupującego.
3. Strony umowy postanawiają, że należności wynikające z niniejszej umowy nie mogą być przedmiotem przelewu wierzytelności, bez pisemnej zgody Kupującego pod rygorem nieważności (przez przelew wierzytelności strony rozumieją również wszelkiego rodzaju umowy zarządzania wierzytelnością, przejęcia wierzytelności do realizacji, ubezpieczenia wierzytelności itp.).
4. Sprzedający oświadcza, że przyjął do wiadomości, iż w trakcie realizacji umowy mogą wystąpić opóźnienia w realizacji zobowiązań ze strony Kupującego, do 90 dni po terminie płatności faktur.

§ 4

1. Sprzedający zapłaci na rzecz Kupującego kary umowne w wypadku:

* zwłoki w realizacji zobowiązań Sprzedawcy – w wysokości 0,5 % wartości przedmiotu sprzedaży określonej w § 2 ust. 1 umowy, za każdy rozpoczęty dzień opóźnienia,

1. Jeżeli szkoda rzeczywista będzie wyższa niż kara umowna, Sprzedający może być zobowiązany do zapłaty odszkodowania przekraczającego karę umowną na zasadach ogólnych.
2. Kupujący może odstąpić od naliczania kar umownych na podstawie pisemnego, uzasadnionego wniosku Sprzedającego.
3. Kupujący zobowiązany jest zobowiązane są do zapłaty kwot wynikających z § 4 umowy w terminie 30 dni od dnia wezwania do zapłaty. Opóźnienie upoważnia Kupującego do naliczenia odsetek ustawowych. W przypadku niedotrzymania terminu określonego w wezwaniu do zapłaty Kupujący ma prawo potrącić należną kwotę wraz z odsetkami z bieżących należności Sprzedającego.
4. Realizacja kar umownych nie wyklucza podejmowania innych działań przez strony umowy, przewidzianych w umowie lub przepisach Kodeksu cywilnego, zmierzających do usunięcia uciążliwości związanych z niewykonywaniem zobowiązań wynikających z umowy.
5. Łączna wysokość kar umownych, które mogą dochodzić strony nie może przekroczyć 50% wartości brutto zawartej umowy.

§ 5

1. Wszelkie zmiany niniejszej umowy wymagają zgodnego oświadczenia stron umowy i formy pisemnej pod rygorem nieważności, chyba że umowa stanowi inaczej.
2. W razie opóźnienia w wykonaniu zamówienia Kupujący ma prawo odstąpić od umowy bez potrzeby udzielania dodatkowego terminu. Wyznaczenie przez Kupującego nowego terminu nie zwalnia Sprzedającego od obowiązku zapłaty kar umownych.
3. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie w chwili zawarcia umowy, Kupujący może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Sprzedający może jedynie żądać wynagrodzenia należnego mu z tytułu wykonanej części umowy.
4. Kupujący zastrzega sobie prawo rezygnacji z zakupu części przedmiotu sprzedaży. Sprzedającemu nie przysługują z tego tytułu roszczenia odszkodowawcze. Kupujący deklaruje realizację co najmniej 70 % wartości umowy.
5. W sprawach nie unormowanych w umowie będą miały zastosowanie przepisy ustawy Prawo zamówień publicznych i Kodeksu Cywilnego.
6. Ewentualne spory powstałe w związku z realizacją umowy rozstrzygane będą przez Sąd właściwy dla siedziby Kupującego.
7. Umowa została spisana w dwóch egzemplarzach, po jednym dla każdej ze stron.

***Sprzedający Kupujący***